National Critical Information Infrastructure Protection Centre

CVE Report

CV Scoring Scale : 3-10 15 May –15 Jun 2018 Vol. 05 No.11

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
Application					
Dolibarr					
Dolibarr					
XSS	22-05-2018	**4.3**	Cross-site scripting (XSS) vulnerability in Dolibarr before 7.0.2 allows remote attackers to inject arbitrary web script or HTML via the foruserlogin parameter to adherents/cartes/carte.php.**CVE-ID:CVE-2018-10095**	https://sysdream.com/news/lab/2018-05-21-cve-2018-10095-dolibarr-xss-injection-vulnerability/ https://github.com/Dolibarr/dolibarr/commit/1dc466e1fb687cfe647de4af891720419823ed56 https://github.com/Dolibarr/dolibarr/blob/7.0.2/ChangeLog	**A-Dol-Dolib/18-06-18/1**
Foxitsoftware					
Foxit Reader					
Execute Code Gain Information	17-05-2018	**4.3**	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of U3D files. The issue results from the lack of proper validation of user-supplied data which can result in a read past the end of an allocated data structure. An attacker can leverage this in conjunction with other	https://zerodayinitiative.com/advisories/ZDI-18-381 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/2**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			vulnerabilities to execute code in the context of the context process. Was ZDI-CAN-5494. **CVE-ID:CVE-2018-9983**		
Foxit Reader, Phantom Pdf					
Execute Code	17-05-2018	**6.8**	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the addLink method.** The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5379. **CVE-ID:CVE-2018-9944**	https://zerodayinitiative.com/advisories/ZDI-18-328 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/3**
Execute Code	17-05-2018	**6.8**	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the AFSimple_Calculate method.** The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5491. **CVE-ID:CVE-2018-1180**	https://zerodayinitiative.com/advisories/ZDI-18-318 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/4**

CV Scoring Scale (CVSS)	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
Execute Code	17-05-2018	**6.8**	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the getField method.** The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5382. **CVE-ID:CVE-2018-9945**	https://zerodayinitiative.com/advisories/ZDI-18-329 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/5**
Execute Code	17-05-2018	**6.8**	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the handling of CPDF_Object objects.** The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5414. **CVE-ID:CVE-2018-9951**	https://zerodayinitiative.com/advisories/ZDI-18-335 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/6**
Execute Code	17-05-2018	**6.8**	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the	https://zerodayinitiative.com/advisories/ZDI-18-323 https://www.foxitsoftware.com/support/security-	**A-Fox-Foxit/18-06-18/7**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			target must visit a malicious page or open a malicious file. **The specific flaw exists within the handling of layout elements.** The issue results from the lack of proper validation of user-supplied data which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5373. **CVE-ID:CVE-2018-9939**	bulletins.php	
Execute Code	17-05-2018	**6.8**	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the handling of the absPageSpan method.** The issue results from the lack of proper validation of user-supplied data which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5372. **CVE-ID:CVE-2018-9938**	https://zerodayinitiative.com/advisories/ZDI-18-322 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/8**
Execute Code	17-05-2018	**6.8**	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the handling of the addAnnot**	https://zerodayinitiative.com/advisories/ZDI-18-315 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/9**

CV Scoring Scale (CVSS)	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			method. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5488. **CVE-ID:CVE-2018-1177**		
Execute Code	17-05-2018	**6.8**	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the handling of the addField method.** The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5489. **CVE-ID:CVE-2018-1178**	https://zerodayinitiative.com/advisories/ZDI-18-316 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/10**
Execute Code	17-05-2018	**6.8**	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the handling of the layout sheet attribute.** The issue results from the lack of proper validation of user-supplied data which can result in a type confusion condition. An attacker can	https://zerodayinitiative.com/advisories/ZDI-18-324 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/11**

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			leverage this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5374. **CVE-ID:CVE-2018-9940**		
Execute Code	17-05-2018	**6.8**	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the handling of the openList method.** The issue results from the lack of proper validation of user-supplied data which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5377. **CVE-ID:CVE-2018-9943**	https://zerodayinitiative.com/advisories/ZDI-18-327 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/12**
Execute Code	17-05-2018	**6.8**	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the handling of the record append method.** The issue results from the lack of proper validation of user-supplied data which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code under the context of the current process. Was ZDI-	https://zerodayinitiative.com/advisories/ZDI-18-325 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/13**

CV Scoring Scale (CVSS)	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			CAN-5375. **CVE-ID:CVE-2018-9941**		
Execute Code	17-05-2018	**6.8**	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the handling of the record remove method.** The issue results from the lack of proper validation of user-supplied data which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5376. **CVE-ID:CVE-2018-9942**	https://zerodayinitiative.com/advisories/ZDI-18-326 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/14**
Execute Code	17-05-2018	**6.8**	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the handling of the XFA borderColor attribute.** The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5436. **CVE-ID:CVE-2018-1173**	https://zerodayinitiative.com/advisories/ZDI-18-311 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/15**

CV Scoring Scale (CVSS)	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
Execute Code	17-05-2018	**6.8**	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the parsing of ePub files.** The issue results from the lack of proper validation of user-supplied data which can result in a write past the end of an allocated object. An attacker can leverage this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5442. **CVE-ID:CVE-2018-1176**	https://zerodayinitiative.com/advisories/ZDI-18-314 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/16**
Execute Code	17-05-2018	**6.8**	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the parsing of field elements.** The issue results from the lack of proper validation of user-supplied data which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5370. **CVE-ID:CVE-2018-9936**	https://zerodayinitiative.com/advisories/ZDI-18-320 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/17**
Execute Code	17-05-2018	**6.8**	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit	https://zerodayinitiative.com/advisories/ZDI-18-400 https://www.foxits	**A-Fox-Foxit/18-06-18/18**

CV Scoring Scale (CVSS)	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the parsing of JPEG images embedded inside U3D files.** The issue results from the lack of proper validation of user-supplied data which can result in a memory access past the end of an allocated data structure. An attacker can leverage this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5422. **CVE-ID:CVE-2018-10490**	oftware.com/support/security-bulletins.php	
Execute Code	17-05-2018	**6.8**	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the parsing of Modifier Chain objects in U3D files.** The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5427. **CVE-ID:CVE-2018-9977**	https://zerodayinitiative.com/advisories/ZDI-18-375 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/19**
Execute Code	17-05-2018	**6.8**	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The**	https://zerodayinitiative.com/advisories/ZDI-18-405 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/20**

CV Scoring Scale (CVSS)	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			specific flaw exists within the parsing of PDF documents. The issue results from the lack of proper validation of user-supplied data which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5586. **CVE-ID:CVE-2018-10495**		
Execute Code	17-05-2018	**6.8**	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the parsing of subform elements.** The issue results from the lack of proper validation of user-supplied data which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5371. **CVE-ID:CVE-2018-9937**	https://zerodayinitiative.com/advisories/ZDI-18-321 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/21**
Execute Code	17-05-2018	**6.8**	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the parsing of the Texture Width in U3D files.** The issue results from the lack of proper validation of user-supplied data which can	https://zerodayinitiative.com/advisories/ZDI-18-380 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/22**

CV Scoring Scale (CVSS)	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			result in a write past the end of an allocated object. An attacker can leverage this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5483. **CVE-ID:CVE-2018-9982**		
Execute Code	17-05-2018	**6.8**	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the parsing of U3D Bone Weight Modifier structures.** The issue results from the lack of proper validation of user-supplied data which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5423. **CVE-ID:CVE-2018-10491**	https://zerodayinitiative.com/advisories/ZDI-18-401 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/23**
Execute Code	17-05-2018	**6.8**	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the parsing of U3D Chain Index objects.** The issue results from the lack of proper validation of user-supplied data which can result in a write past the end of an allocated object. An attacker can leverage this vulnerability to	https://zerodayinitiative.com/advisories/ZDI-18-387 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/24**

CV Scoring Scale (CVSS)	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**
Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;							

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			execute code under the context of the current process. Was ZDI-CAN-5396. **CVE-ID:CVE-2018-10477**		
Execute Code	17-05-2018	**6.8**	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the parsing of U3D CLOD Base Mesh Continuation structures.** The issue results from the lack of proper validation of user-supplied data which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5392. **CVE-ID:CVE-2018-10473**	https://zerodayinitiative.com/advisories/ZDI-18-383 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/25**
Execute Code	17-05-2018	**6.8**	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the parsing of U3D Clod Progressive Mesh Declaration structures**. The issue results from the lack of proper validation of user-supplied data which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code	https://zerodayinitiative.com/advisories/ZDI-18-399 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/26**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			under the context of the current process. Was ZDI-CAN-5421. **CVE-ID:CVE-2018-10489**		
Execute Code	17-05-2018	**6.8**	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the parsing of U3D Clod Progressive Mesh objects.** The issue results from the lack of proper validation of user-supplied data which can result in a write past the end of an allocated object. An attacker can leverage this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5410. **CVE-ID:CVE-2018-10483**	https://zerodayinitiative.com/advisories/ZDI-18-393 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/27**
Execute Code	17-05-2018	**6.8**	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the parsing of U3D files.** The issue results from the lack of proper initialization of a pointer prior to accessing it. An attacker can leverage this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5431. **CVE-ID:CVE-2018-9981**	https://zerodayinitiative.com/advisories/ZDI-18-379 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/28**

CV Scoring Scale (CVSS)	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
Execute Code	17-05-2018	**6.8**	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the parsing of U3D Node objects.** The issue results from the lack of proper initialization of a pointer prior to accessing it. An attacker can leverage this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5411. **CVE-ID:CVE-2018-10484**	https://zerodayinitiative.com/advisories/ZDI-18-394 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/29**
Execute Code	17-05-2018	**6.8**	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the parsing of U3D Shading objects.** The issue results from the lack of proper validation of user-supplied data which can result in a write past the end of an allocated object. An attacker can leverage this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5393. **CVE-ID:CVE-2018-10474**	https://zerodayinitiative.com/advisories/ZDI-18-384 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/30**
Execute Code	17-05-2018	**6.8**	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.1.1049. User interaction is required to exploit	https://zerodayinitiative.com/advisories/ZDI-18-350 https://www.foxits	**A-Fox-Foxit/18-06-18/31**

CV Scoring Scale (CVSS)	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the handling of Calculate actions of TextBox objects.** The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5570. **CVE-ID:CVE-2018-9966**	oftware.com/support/security-bulletins.php	
Execute Code	17-05-2018	**6.8**	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.1.1049. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the handling of Format actions of TextBox objects.** The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5571. **CVE-ID:CVE-2018-9967**	https://zerodayinitiative.com/advisories/ZDI-18-351 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/32**
Execute Code	17-05-2018	**6.8**	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.1.1049. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the handling of Keystroke actions**	https://zerodayinitiative.com/advisories/ZDI-18-352 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/33**

CV Scoring Scale (CVSS)	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			of TextBox objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5572. **CVE-ID:CVE-2018-9968**		
Execute Code	17-05-2018	**6.8**	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.1.1049. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the handling of shift events.** The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5762. **CVE-ID:CVE-2018-9975**	https://zerodayinitiative.com/advisories/ZDI-18-359 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/34**
Execute Code	17-05-2018	**6.8**	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.1.1049. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the handling of Text Annotations.** When setting the point attribute the process does not properly validate the existence of an object prior to performing operations on the object. An attacker can	https://zerodayinitiative.com/advisories/ZDI-18-342 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/35**

CV Scoring Scale (CVSS)	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**
Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;							

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			leverage this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5620. **CVE-ID:CVE-2018-9958**		
Execute Code	17-05-2018	**6.8**	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.1.1049. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the handling of the setAction method of Link objects.** The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5569. **CVE-ID:CVE-2018-9965**	https://zerodayinitiative.com/advisories/ZDI-18-349 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/36**
Execute Code	17-05-2018	**6.8**	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.1.1049. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the handling of XFA Button elements.** When parsing arguments passed to the resetDatamethod the process does not properly validate the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code	https://zerodayinitiative.com/advisories/ZDI-18-341 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/37**

CV Scoring Scale (CVSS)	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**
Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;							

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			under the context of the current process. Was ZDI-CAN-5618. **CVE-ID:CVE-2018-9957**		
Execute Code	17-05-2018	**6.8**	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.1.1049. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the handling of XFA Button elements.** When setting the formatted Value attribute the process does not properly validate the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5527. **CVE-ID:CVE-2018-9952**	https://zerodayinitiative.com/advisories/ZDI-18-336 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/38**
Execute Code	17-05-2018	**6.8**	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.1.1049. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the handling of XFA Button elements.** When setting the title attribute the process does not properly validate the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5617.	https://zerodayinitiative.com/advisories/ZDI-18-340 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/39**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			CVE-ID:CVE-2018-9956		
Execute Code	17-05-2018	**6.8**	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.1.1049. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the handling of XFA Button elements.** When setting the y attribute the process does not properly validate the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5529. **CVE-ID:CVE-2018-9954**	https://zerodayinitiative.com/advisories/ZDI-18-338 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/40**
Execute Code	17-05-2018	**6.8**	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.1.1049. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the parsing of Annotation's author attribute.** The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5435.	https://zerodayinitiative.com/advisories/ZDI-18-346 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/41**

CV Scoring Scale (CVSS)	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			CVE-ID:CVE-2018-9962		
Execute Code	17-05-2018	**6.8**	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.1.1049. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the parsing of the name attribute of OCG objects.** The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5568. **CVE-ID:CVE-2018-9964**	https://zerodayinitiative.com/advisories/ZDI-18-348 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/42**
Execute Code	17-05-2018	**6.8**	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.1.1049. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the parsing of the pageNum document attribute.** The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5432. **CVE-ID:CVE-2018-9959**	https://zerodayinitiative.com/advisories/ZDI-18-343 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/43**

CV Scoring Scale (CVSS)	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
Execute Code	17-05-2018	**6.8**	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.1.1049. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the parsing of the rect Field attribute.** The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5434. **CVE-ID:CVE-2018-9961**	https://zerodayinitiative.com/advisories/ZDI-18-345 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/44**
Execute Code	17-05-2018	**6.8**	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.1.1049. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the parsing of the textColor Field attribute.** The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5433. **CVE-ID:CVE-2018-9960**	https://zerodayinitiative.com/advisories/ZDI-18-344 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/45**
Execute Code	17-05-2018	**6.8**	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.1.1049. User interaction is required to exploit	https://zerodayinitiative.com/advisories/ZDI-18-353 https://www.foxits	**A-Fox-Foxit/18-06-18/46**

CV Scoring Scale (CVSS)	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the XFA boundItem method of Button elements.** The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5579. **CVE-ID:CVE-2018-9969**	oftware.com/support/security-bulletins.php	
Execute Code	17-05-2018	**6.8**	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.1.1049. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the XFA resolveNode method of Button elements.** The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5531. **CVE-ID:CVE-2018-9955**	https://zerodayinitiative.com/advisories/ZDI-18-339 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/47**
Execute Code	17-05-2018	**6.8**	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.1.1049. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the XFA resolveNodes method of**	https://zerodayinitiative.com/advisories/ZDI-18-337 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/48**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			Button elements. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5528. **CVE-ID:CVE-2018-9953**		
Execute Code Gain Information	17-05-2018	**4.3**	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the handling of the bitmapDPI attribute of PrintParams objects.** The issue results from the lack of proper initialization of memory prior to accessing it. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-5437. **CVE-ID:CVE-2018-1174**	https://zerodayinitiative.com/advisories/ZDI-18-312 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/49**
Execute Code Gain Information	17-05-2018	**4.3**	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the handling of the interactive attribute of PrintParams objects.** The issue results from	https://zerodayinitiative.com/advisories/ZDI-18-313 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/50**

CV Scoring Scale (CVSS)	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			the lack of proper initialization of memory prior to accessing it. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-5438. **CVE-ID:CVE-2018-1175**		
Execute Code Gain Information	17-05-2018	**4.3**	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the handling of the setTimeOut method.** The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-5471. **CVE-ID:CVE-2018-9946**	https://zerodayinitiative.com/advisories/ZDI-18-330 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/51**
Execute Code Gain Information	17-05-2018	**4.3**	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the handling of the U3D Node Name buffer.** The issue results from the lack of proper validation of user-supplied data which can	https://zerodayinitiative.com/advisories/ZDI-18-390 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/52**

CV Scoring Scale (CVSS)	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-5401. **CVE-ID:CVE-2018-10480**		
Execute Code Gain Information	17-05-2018	**4.3**	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the handling of typed arrays.** The issue results from the lack of proper initialization of a pointer prior to accessing it. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-5380. **CVE-ID:CVE-2018-9948**	https://zerodayinitiative.com/advisories/ZDI-18-332 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/53**
Execute Code Gain Information	17-05-2018	**4.3**	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the handling of U3D Texture Resource structures.** The issue results from the lack of proper validation of user-supplied data which can result in a read past the end of an allocated data structure. An attacker can	https://zerodayinitiative.com/advisories/ZDI-18-391 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/54**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-5408. **CVE-ID:CVE-2018-10481**		
Execute Code Gain Information	17-05-2018	**4.3**	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the parsing of DataSubBlock structures in GIF images.** The issue results from the lack of proper validation of user-supplied data which can result in a read past the end of an allocated data structure. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-5490. **CVE-ID:CVE-2018-1179**	https://zerodayinitiative.com/advisories/ZDI-18-317 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/55**
Execute Code Gain Information	17-05-2018	**4.3**	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the parsing of PDF documents.** The issue results from the lack of proper validation of user-supplied data which can result in a read past the end of an	https://zerodayinitiative.com/advisories/ZDI-18-334 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/56**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-5413. **CVE-ID:CVE-2018-9950**		
Execute Code Gain Information	17-05-2018	**4.3**	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the parsing of Texture Continuation objects in U3D files.** The issue results from the lack of proper validation of user-supplied data which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-5429. **CVE-ID:CVE-2018-9979**	https://zerodayinitiative.com/advisories/ZDI-18-377 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/57**
Execute Code Gain Information	17-05-2018	**4.3**	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the parsing of Texture Image Channels objects in U3D files.** The issue results from the lack of proper validation of user-supplied data which can result in	https://zerodayinitiative.com/advisories/ZDI-18-382 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/58**

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-5495. **CVE-ID:CVE-2018-9984**		
Execute Code Gain Information	17-05-2018	**4.3**	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the parsing of Texture objects in U3D files.** The issue results from the lack of proper validation of user-supplied data which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-5425. **CVE-ID:CVE-2018-9976**	https://zerodayinitiative.com/advisories/ZDI-18-374 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/59**
Execute Code Gain Information	17-05-2018	**4.3**	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the parsing of the U3D Image Index.** The issue results from the lack of proper validation of user-supplied data which can result in a read past the end of an	https://zerodayinitiative.com/advisories/ZDI-18-396 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/60**

CV Scoring Scale (CVSS)	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-5418. **CVE-ID:CVE-2018-10486**		
Execute Code Gain Information	17-05-2018	**4.3**	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the parsing of U3D Clod Progressive Mesh Continuation structures.** The issue results from the lack of proper validation of user-supplied data which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-5424. **CVE-ID:CVE-2018-10492**	https://zerodayinitiative.com/advisories/ZDI-18-402 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/61**
Execute Code Gain Information	17-05-2018	**4.3**	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the parsing of U3D files embedded inside PDF documents.** The issue results from the lack of proper validation of user-supplied data which can result in	https://zerodayinitiative.com/advisories/ZDI-18-397 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/62**

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-5419. **CVE-ID:CVE-2018-10487**		
Execute Code Gain Information	17-05-2018	**4.3**	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the parsing of U3D files.** The issue results from the lack of proper validation of user-supplied data which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the context process. Was ZDI-CAN-5428. **CVE-ID:CVE-2018-9978**	https://zerodayinitiative.com/advisories/ZDI-18-376 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/63**
Execute Code Gain Information	17-05-2018	**4.3**	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the parsing of U3D files.** The issue results from the lack of proper validation of user-supplied data which can result in a read past the end of an allocated object. An	https://zerodayinitiative.com/advisories/ZDI-18-378 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/64**

CV Scoring Scale (CVSS)	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-5430. **CVE-ID:CVE-2018-9980**		
Execute Code Gain Information	17-05-2018	**4.3**	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the parsing of U3D Key Frame structures.** The issue results from the lack of proper validation of user-supplied data which can result in a read past the end of an allocated data structure. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-5399. **CVE-ID:CVE-2018-10479**	https://zerodayinitiative.com/advisories/ZDI-18-389 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/65**
Execute Code Gain Information	17-05-2018	**4.3**	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the parsing of U3D Light Node structures.** The issue results from the lack of proper validation of user-supplied data which can result in a read past the end of an	https://zerodayinitiative.com/advisories/ZDI-18-385 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/66**

CV Scoring Scale (CVSS)	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			allocated structure. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-5394. **CVE-ID:CVE-2018-10475**		
Execute Code Gain Information	17-05-2018	**4.3**	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the parsing of U3D Model Node structures.** The issue results from the lack of proper validation of user-supplied data which can result in a read past the end of an allocated structure. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-5395. **CVE-ID:CVE-2018-10476**	https://zerodayinitiative.com/advisories/ZDI-18-386 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/67**
Execute Code Gain Information	17-05-2018	**4.3**	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the parsing of U3D Texture Coord Dimensions objects.** The issue results from the lack of proper validation of user-supplied data which can result in a read past the end of an allocated object. An	https://zerodayinitiative.com/advisories/ZDI-18-388 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/68**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-5397. **CVE-ID:CVE-2018-10478**		
Execute Code Gain Information	17-05-2018	**4.3**	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the U3D Texture Image Format object.** The issue results from the lack of proper validation of user-supplied data which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-5409. **CVE-ID:CVE-2018-10482**	https://zerodayinitiative.com/advisories/ZDI-18-392 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/69**
Execute Code Gain Information	17-05-2018	**4.3**	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within U3D Texture Height structures.** The issue results from the lack of proper validation of user-supplied data which can result in a read past the end of an allocated data structure. An	https://zerodayinitiative.com/advisories/ZDI-18-395 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/70**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-5412. **CVE-ID:CVE-2018-10485**		
Execute Code Gain Information	17-05-2018	**4.3**	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 9.0.1.1049. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within ConvertToPDF_x86.dll.** The issue results from the lack of proper validation of user-supplied data which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-5755. **CVE-ID:CVE-2018-9972**	https://zerodayinitiative.com/advisories/ZDI-18-356 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/71**
Execute Code Gain Information	17-05-2018	**4.3**	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 9.0.1.1049. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the parsing of ePub files.** The issue results from the lack of proper validation of user-supplied data which can result in a read past the end of an allocated buffer. An	https://zerodayinitiative.com/advisories/ZDI-18-357 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/72**

CV Scoring Scale (CVSS)	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-5758. **CVE-ID:CVE-2018-9973**		
Execute Code Gain Information	17-05-2018	**4.3**	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 9.0.1.1049. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the parsing of JPEG2000 images.** The issue results from the lack of proper validation of user-supplied data which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-5549. **CVE-ID:CVE-2018-9963**	https://zerodayinitiative.com/advisories/ZDI-18-347 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/73**
Execute Code Gain Information	17-05-2018	**4.3**	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 9.0.1.1049. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the parsing of the U3D Final Maximum Resolution attribute.** The issue results from the lack of proper validation of user-supplied data which can result in	https://zerodayinitiative.com/advisories/ZDI-18-403 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/74**

CV Scoring Scale (CVSS)	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-5426. **CVE-ID:CVE-2018-10493**		
Execute Code Overflow	17-05-2018	**6.8**	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the parsing of BMP images.** The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length heap-based buffer. An attacker can leverage this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5472. **CVE-ID:CVE-2018-9947**	https://zerodayinitiative.com/advisories/ZDI-18-331 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/75**
Execute Code Overflow	17-05-2018	**6.8**	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the parsing of TIFF files.** The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length heap-based buffer. An attacker can leverage this vulnerability to execute code	https://zerodayinitiative.com/advisories/ZDI-18-333 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/76**

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			under the context of the current process. Was ZDI-CAN-5473. **CVE-ID:CVE-2018-9949**		
Execute Code Overflow	17-05-2018	**6.8**	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.0.29935. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the parsing of U3D Texture Width structures.** The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length heap-based buffer. An attacker can leverage this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5420. **CVE-ID:CVE-2018-10488**	https://zerodayinitiative.com/advisories/ZDI-18-398 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/77**
Execute Code Overflow	17-05-2018	**6.8**	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.1.1049. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within ConvertToPDF_x86.dll.** The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-5895. **CVE-ID:CVE-2018-9974**	https://zerodayinitiative.com/advisories/ZDI-18-358 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/78**

CV Scoring Scale (CVSS)	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
Execute Code Overflow	17-05-2018	**6.8**	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.0.1.1049. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the parsing of U3D 3DView objects.** The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5493. **CVE-ID:CVE-2018-10494**	https://zerodayinitiative.com/advisories/ZDI-18-404 https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Foxit/18-06-18/79**
PhantompdfReader					
Execute Code	24-05-2018	**6.8**	An issue was discovered in Foxit Reader before 9.1 and PhantomPDF before 9.1. This vulnerability allows remote attackers to execute arbitrary code. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists when rendering U3D images inside of pdf files**. The issue results from the lack of proper validation of user-supplied data which can result in a type confusion condition. An attacker can leverage this to execute code in the context of the current process. **CVE-ID:CVE-2018-7407**	https://srcincite.io/advisories/src-2018-0018/ https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Phant/18-06-18/80**
Execute Code	24-05-2018	**6.8**	An issue was discovered in Foxit Reader before 9.1 and	https://srcincite.io/advisories/src-	**A-Fox-Phant/18-**

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			PhantomPDF before 9.1. This vulnerability allows remote attackers to execute arbitrary code. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the u3d images inside of a pdf.** The issue results from the lack of proper validation of user-supplied data which can result in an array indexing issue. An attacker can leverage this to execute code in the context of the current process. **CVE-ID:CVE-2018-7406**	2018-0017/ https://www.foxitsoftware.com/support/security-bulletins.php	**06-18/81**
Execute Code	24-05-2018	**6.8**	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader before 9.1 and PhantomPDF before 9.1. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the processing of specially crafted pdf files with embedded u3d images.** Crafted data in the PDF file can trigger an out-of-bounds write on a buffer. An attacker can leverage this vulnerability to execute code under the context of the current process. **CVE-ID:CVE-2018-5675**	https://srcincite.io/advisories/src-2018-0013/ https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Phant/18-06-18/82**
Execute Code	24-05-2018	**6.8**	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader before 9.1 and PhantomPDF before 9.1. User interaction is required to exploit this vulnerability in that the	https://srcincite.io/advisories/src-2018-0016/ https://www.foxitsoftware.com/support/security-	**A-Fox-Phant/18-06-18/83**

CV Scoring Scale (CVSS)	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**
Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;							

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			target must visit a malicious page or open a malicious file. **The specific flaw exists within the processing of specially crafted pdf files with embedded u3d images.** The issue results from the lack of proper validation of user-supplied data which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process a different vulnerability than CVE-2018-5677 and CVE-2018-5679. **CVE-ID:CVE-2018-5680**	bulletins.php	
Execute Code	24-05-2018	**6.8**	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader before 9.1 and PhantomPDF before 9.1. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the processing of specially crafted pdf files with embedded u3d images.** The issue results from the lack of proper validation of user-supplied data which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process a different vulnerability than CVE-2018-5677 and CVE-2018-5680. **CVE-ID:CVE-2018-5679**	https://srcincite.io/advisories/src-2018-0015/ https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Phant/18-06-18/84**
Execute Code	24-05-2018	**6.8**	This vulnerability allows remote attackers to execute arbitrary	https://srcincite.io/advisories/src-	**A-Fox-Phant/18-**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;							

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			code on vulnerable installations of Foxit Reader before 9.1 and PhantomPDF before 9.1. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the processing of specially crafted pdf files with embedded u3d images.** The issue results from the lack of proper validation of user-supplied data which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process a different vulnerability than CVE-2018-5679 and CVE-2018-5680. **CVE-ID:CVE-2018-5677**	2018-0014/ https://www.foxitsoftware.com/support/security-bulletins.php	**06-18/85**
Execute Code Overflow	24-05-2018	**6.8**	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader before 9.1 and PhantomPDF before 9.1. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the processing of specially crafted pdf files with embedded u3d images.** Crafted data in the PDF file can trigger an overflow of a heap-based buffer. An attacker can leverage this vulnerability to execute code under the context of the current process a different vulnerability than CVE-2018-5674 and CVE-2018-5676. **CVE-ID:CVE-2018-5678**	https://srcincite.io/advisories/src-2018-0012/ https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Phant/18-06-18/86**

CV Scoring Scale (CVSS)	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
Execute Code Overflow	24-05-2018	**6.8**	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader before 9.1 and PhantomPDF before 9.1. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the processing of specially crafted pdf files with embedded u3d images.** Crafted data in the PDF file can trigger an overflow of a heap-based buffer. An attacker can leverage this vulnerability to execute code under the context of the current process a different vulnerability than CVE-2018-5674 and CVE-2018-5678. **CVE-ID:CVE-2018-5676**	https://srcincite.io/advisories/src-2018-0011/ https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Phant/18-06-18/87**
Execute Code Overflow	24-05-2018	**6.8**	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader before 9.1 and PhantomPDF before 9.1. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **The specific flaw exists within the processing of specially crafted pdf files with embedded u3d images.** Crafted data in the PDF file can trigger an overflow of a heap-based buffer. An attacker can leverage this vulnerability to execute code under the context of the current process a different vulnerability than CVE-2018-5676 and CVE-2018-5678. **CVE-ID:CVE-2018-5674**	https://srcincite.io/advisories/src-2018-0010/ https://www.foxitsoftware.com/support/security-bulletins.php	**A-Fox-Phant/18-06-18/88**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
Hdfgroup					
Hdf5					
DoS	16-05-2018	**4.3**	A division by zero was discovered in H5D__btree_decode_key in H5Dbtree.c in the HDF HDF5 1.10.2 library. It could allow a remote denial of service attack. **CVE-ID:CVE-2018-11203**	https://github.com/Twi1ight/fuzzing-pocs/tree/master/hdf5	**A-Hdf-Hdf5/18-06-18/89**
DoS	16-05-2018	**4.3**	A division by zero was discovered in H5D__chunk_init in H5Dchunk.c in the HDF HDF5 1.10.2 library. It could allow a remote denial of service attack. **CVE-ID:CVE-2018-11207**	https://github.com/Twi1ight/fuzzing-pocs/tree/master/hdf5	**A-Hdf-Hdf5/18-06-18/90**
DoS	16-05-2018	**4.3**	A NULL pointer dereference was discovered in H5O__chunk_deserialize in H5Ocache.c in the HDF HDF5 1.10.2 library. It could allow a remote denial of service attack. **CVE-ID:CVE-2018-11204**	https://github.com/Twi1ight/fuzzing-pocs/tree/master/hdf5	**A-Hdf-Hdf5/18-06-18/91**
DoS	16-05-2018	**5.8**	A out of bounds read was discovered in H5O_fill_new_decode and H5O_fill_old_decode in H5Ofill.c in the HDF HDF5 1.10.2 library. It could allow a remote denial of service or information disclosure attack. **CVE-ID:CVE-2018-11206**	https://github.com/Twi1ight/fuzzing-pocs/tree/master/hdf5	**A-Hdf-Hdf5/18-06-18/92**
DoS	16-05-2018	**5.8**	A out of bounds read was discovered in H5VM_memcpyvv in H5VM.c in the HDF HDF5 1.10.2 library. It could allow a remote denial of service or information disclosure attack. **CVE-ID:CVE-2018-11205**	https://github.com/Twi1ight/fuzzing-pocs/tree/master/hdf5	**A-Hdf-Hdf5/18-06-18/93**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
IBM					
Spectrum Virtualize For Public Cloud SoftwareSpectrum Virtualize SoftwareStorwize V3500 SoftwareStorwize V3700 SoftwareStorwize V5000 SoftwareStorwize V7000 Software					
CSRF	17-05-2018	**6.8**	IBM SAN Volume Controller IBM Storwize IBM Spectrum Virtualize and IBM FlashSystem products (6.1 6.2 6.3 6.4 7.1 7.2 7.3 7.4 7.5 7.6 7.6.1 7.7 7.7.1 7.8 7.8.1 8.1 and 8.1.1) are vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID **CVE-ID:CVE-2018-1434**	https://exchange.xforce.ibmcloud.com/vulnerabilities/139474	**A-IBM-Spect/18-06-18/94**
DoS	17-05-2018	**6.5**	IBM SAN Volume Controller IBM Storwize IBM Spectrum Virtualize and IBM FlashSystem products (6.1 6.2 6.3 6.4 7.1 7.2 7.3 7.4 7.5 7.6 7.6.1 7.7 7.7.1 7.8 7.8.1 8.1 and 8.1.1) could allow an authenticated user to access system files they should not have access to including deleting files or causing a denial of service. IBM X-Force ID **CVE-ID:CVE-2018-1462**	https://exchange.xforce.ibmcloud.com/vulnerabilities/140363	**A-IBM-Spect/18-06-18/95**
Gain Information	17-05-2018	**3.5**	IBM SAN Volume Controller IBM Storwize IBM Spectrum Virtualize and IBM FlashSystem products (6.1 6.2 6.3 6.4 7.1 7.2 7.3 7.4 7.5 7.6 7.6.1 7.7 7.7.1 7.8 7.8.1 8.1 and 8.1.1) could allow an authenticated user to obtain the private key which could make intercepting GUI communications possible. IBM X-Force ID **CVE-ID:CVE-2018-1465**	https://exchange.xforce.ibmcloud.com/vulnerabilities/140396	**A-IBM-Spect/18-06-18/96**
Gain Information	17-05-2018	**4**	IBM SAN Volume Controller IBM Storwize IBM Spectrum Virtualize and IBM FlashSystem products (6.1 6.2 6.3 6.4 7.1 7.2 7.3 7.4 7.5	https://exchange.xforce.ibmcloud.com/vulnerabilities/140395	**A-IBM-Spect/18-06-18/97**

CV Scoring Scale (CVSS)	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**
Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;							

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			7.6 7.6.1 7.7 7.7.1 7.8 7.8.1 8.1 and 8.1.1) could allow an authenticated user to obtain sensitive information that they should not have authorization to read. IBM X-Force ID **CVE-ID:CVE-2018-1464**		
Gain Information	17-05-2018	**5**	IBM SAN Volume Controller IBM Storwize IBM Spectrum Virtualize and IBM FlashSystem products (6.1 6.2 6.3 6.4 7.1 7.2 7.3 7.4 7.5 7.6 7.6.1 7.7 7.7.1 7.8 7.8.1 8.1 and 8.1.1) web handler /DLSnap could allow an unauthenticated attacker to read arbitrary files on the system. IBM X-Force ID **CVE-ID:CVE-2018-1438**	https://exchange.xforce.ibmcloud.com/vulnerabilities/139566	**A-IBM-Spect/18-06-18/98**
Gain Information	17-05-2018	**5**	IBM SAN Volume Controller IBM Storwize IBM Spectrum Virtualize and IBM FlashSystem products (6.1 6.2 6.3 6.4 7.1 7.2 7.3 7.4 7.5 7.6 7.6.1 7.7 7.7.1 7.8 7.8.1 8.1 and 8.1.1) web handler /DownloadFile does not require authentication to read arbitrary files from the system. IBM X-Force ID **CVE-ID:CVE-2018-1433**	https://exchange.xforce.ibmcloud.com/vulnerabilities/139473	**A-IBM-Spect/18-06-18/99**
NA	17-05-2018	**3.5**	IBM SAN Volume Controller IBM Storwize IBM Spectrum Virtualize and IBM FlashSystem products (6.1 6.2 6.3 6.4 7.1 7.2 7.3 7.4 7.5 7.6 7.6.1 7.7 7.7.1 7.8 7.8.1 8.1 and 8.1.1) use weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID **CVE-ID:CVE-2018-1466**	https://exchange.xforce.ibmcloud.com/vulnerabilities/140397	**A-IBM-Spect/18-06-18/100**
NA	17-05-2018	**4**	IBM SAN Volume Controller IBM Storwize IBM Spectrum Virtualize and IBM FlashSystem products (	https://exchange.xforce.ibmcloud.com/vulnerabilities/140	**A-IBM-Spect/18-06-**

CV Scoring Scale (CVSS)	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			6.1 6.2 6.3 6.4 7.1 7.2 7.3 7.4 7.5 7.6 7.6.1 7.7 7.7.1 7.8 7.8.1 8.1 and 8.1.1) could allow an authenticated user to access system files they should not have access to some of which could contain account credentials. IBM X-Force ID **CVE-ID:CVE-2018-1463**	368	**18/101**
XSS	17-05-2018	**3.5**	IBM SAN Volume Controller IBM Storwize IBM Spectrum Virtualize and IBM FlashSystem products (6.1 6.2 6.3 6.4 7.1 7.2 7.3 7.4 7.5 7.6 7.6.1 7.7 7.7.1 7.8 7.8.1 8.1 and 8.1.1) are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID **CVE-ID:CVE-2018-1461**	https://exchange.xforce.ibmcloud.com/vulnerabilities/140362	**A-IBM-Spect/18-06-18/102**
IJG					
Libjpeg					
DoS	16-05-2018	**4.3**	An issue was discovered in libjpeg 9a. The alloc_sarray function in jmemmgr.c allows remote attackers to cause a denial of service (divide-by-zero error) via a crafted file. **CVE-ID:CVE-2018-11212**	https://github.com/ChijinZ/security_advisories/tree/master/libjpeg-v9a	**A-IJG-Libjp/18-06-18/103**
DoS	16-05-2018	**4.3**	An issue was discovered in libjpeg 9a. The get_text_gray_row function in rdppm.c allows remote attackers to cause a denial of service (Segmentation fault) via a crafted file. **CVE-ID:CVE-2018-11213**	https://github.com/ChijinZ/security_advisories/tree/master/libjpeg-v9a	**A-IJG-Libjp/18-06-18/104**
DoS	16-05-2018	**4.3**	An issue was discovered in libjpeg 9a. The get_text_rgb_row function in rdppm.c allows	https://github.com/ChijinZ/security_advisories/tree/maste	**A-IJG-Libjp/18-06-**

CV Scoring Scale (CVSS)	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			remote attackers to cause a denial of service (Segmentation fault) via a crafted file. **CVE-ID:CVE-2018-11214**	r/libjpeg-v9a	**18/105**
Ilias					
Ilias					
NA	17-05-2018	**5.8**	ILIAS 5.1.x 5.2.x and 5.3.x before 5.3.5 redirects a logged-in user to a third-party site via the return_to_url parameter. **CVE-ID:CVE-2018-11119**	https://www.ilias.de/docu/goto.php?target=st_229https://github.com/ILIAS-eLearning/ILIAS/commit/01a24cf04fe8dddf1da59ca497580637973482b6	**A-Ili-Ilias/18-06-18/106**
XSS	17-05-2018	**4.3**	Services/COPage/classes/class.ilPCSourceCode.php in ILIAS 5.1.x 5.2.x and 5.3.x before 5.3.5 has XSS. **CVE-ID:CVE-2018-11120**	https://www.ilias.de/docu/goto.php?target=st_229https://github.com/ILIAS-eLearning/ILIAS/commit/7959485406eb981976b64fee363cf950603924ed	**A-Ili-Ilias/18-06-18/107**
XSS	17-05-2018	**4.3**	Services/Feeds/classes/class.ilExternalFeedItem.php in ILIAS 5.1.x 5.2.x and 5.3.x before 5.3.5 has XSS via a link attribute. **CVE-ID:CVE-2018-11117**	https://www.ilias.de/docu/goto.php?target=st_229https://github.com/ILIAS-eLearning/ILIAS/commit/ff9bf29858f2dbffe828711a6f8bf37038c00d77	**A-Ili-Ilias/18-06-18/108**
XSS	17-05-2018	**4.3**	The RSS subsystem in ILIAS 5.1.x 5.2.x and 5.3.x before 5.3.5 has XSS via a URI to Services/Feeds/classes/class.ilExternalFeedItem.php. **CVE-ID:CVE-2018-11118**	https://github.com/ILIAS-eLearning/ILIAS/commit/6b2217c31b6974788a5c787413454475687b44bb https://www.ilias.de/docu/goto.php?target=st_229https://github.com/ILIAS-eLearning/ILIAS/commit/d0dcad1b1e7	**A-Ili-Ilias/18-06-18/109**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
				29f694acd0582bc626c7c8e62b519	
Imagemagick					
Imagemagick					
DoS	18-05-2018	**4.3**	In ImageMagick 7.0.7-16 Q16 x86_64 2017-12-25 there is a use-after-free in ReadOneMNGImage in coders/png.c which allows attackers to cause a denial of service via a crafted MNG image file that is mishandled in an MngInfoDiscardObject call. **CVE-ID:CVE-2017-18272**	https://github.com/ImageMagick/ImageMagick/issues/918	**A-Ima-Image/18-06-18/110**
DoS Overflow	18-05-2018	**4.3**	In ImageMagick 7.0.7-23 Q16 x86_64 2018-01-24 there is a heap-based buffer over-read in ReadSUNImage in coders/sun.c which allows attackers to cause a denial of service (application crash in SetGrayscaleImage in MagickCore/quantize.c) via a crafted SUN image file. **CVE-ID:CVE-2018-11251**	https://usn.ubuntu.com/3681-1/https://github.com/ImageMagick/ImageMagick/issues/956https://lists.debian.org/debian-lts-announce/2018/05/msg00012.html	**A-Ima-Image/18-06-18/111**
NA	31-05-2018	**6.8**	In ImageMagick 7.0.7-36 Q16 theReadMATImage function in coders/mat.c allows attackers to cause a use after free via a crafted file. **CVE-ID:CVE-2018-11624**	https://github.com/ImageMagick/ImageMagick/issues/1149	**A-Ima-Image/18-06-18/112**
Overflow	31-05-2018	**6.8**	In ImageMagick 7.0.7-37 Q16SetGrayscaleImage in the quantize.c file allows attackers to cause a heap-based buffer over-read via a crafted file. **CVE-ID:CVE-2018-11625**	https://usn.ubuntu.com/3681-1/https://github.com/ImageMagick/ImageMagick/issues/1156	**A-Ima-Image/18-06-18/113**
Microsoft					
Office For Mac					
Exec Code	23-05-2018	**9.3**	A remote code execution vulnerability exists in Microsoft PowerPoint software when the software fails to properly validate XML content aka "Microsoft	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8176	**A-Mic-Offic/18-06-18/114**

CV Scoring Scale (CVSS)	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
		🟥	PowerPoint Remote Code Execution Vulnerability." This affects Microsoft Office. **CVE-ID:CVE-2018-8176**		
Podofo Project					
Podofo					
DoS	18-05-2018	**4.3**	An issue was discovered in PoDoFo 0.9.5. The function PdfPage**CVE-ID:CVE-2018-11255**	https://bugzilla.redhat.com/show_bug.cgi?id=1575502	**A-Pod-Podof/18-06-18/115**
DoS	18-05-2018	**4.3**	An issue was discovered in PoDoFo 0.9.5. There is an Excessive Recursion in the PdfPagesTree**CVE-ID:CVE-2018-11254**	https://bugzilla.redhat.com/show_bug.cgi?id=1576174	**A-Pod-Podof/18-06-18/116**
Wireshark					
Wireshark					
NA	22-05-2018	**5**	In Wireshark2.6.0 2.4.0 to 2.4.6 and 2.2.0 to 2.2.14 the DNS dissector could crash. This was addressed in epan/dissectors/packet-dns.c by avoiding a NULL pointer dereference for an empty name in an SRV record. **CVE-ID:CVE-2018-11356**	https://www.wireshark.org/security/wnpa-sec-2018-29.html https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=14681 https://code.wireshark.org/review/gitweb?p=wireshark.git;a=commit;h=4425716ddba99374749bd033d9bc0f4add2fb973	**A-Wir-Wires/18-06-18/117**
NA	22-05-2018	**5**	In Wireshark2.6.0 2.4.0 to 2.4.6 and 2.2.0 to 2.2.14 the LTP dissector and other dissectors could consume excessive memory. This was addressed in epan/tvbuff.c by rejecting negative lengths. **CVE-ID:CVE-2018-11357**	https://www.wireshark.org/security/wnpa-sec-2018-28.html https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=14678	**A-Wir-Wires/18-06-18/118**

CV Scoring Scale (CVSS)	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
				https://code.wireshark.org/review/gitweb?p=wireshark.git;a=commit;h=ab8a33ef083b9732c89117747a83a905a676faf6	
NA	22-05-2018	**5**	In Wireshark2.6.0 2.4.0 to 2.4.6 and 2.2.0 to 2.2.14 the Q.931 dissector could crash. This was addressed in epan/dissectors/packet-q931.c by avoiding a use-after-free after a malformed packet prevented certain cleanup. **CVE-ID:CVE-2018-11358**	https://www.wireshark.org/security/wnpa-sec-2018-31.html https://www.debian.org/security/2018/dsa-4217 https://code.wireshark.org/review/gitweb?p=wireshark.git;a=commit;h=ccb1ac3c8cec47fbbbf2e80ced80644005c65252 https://lists.debian.org/debian-lts-announce/2018/05/msg00019.htmlhttps://bugs.wireshark.org/bugzilla/show_bug.cgi?id=14689	**A-Wir-Wires/18-06-18/119**
NA	22-05-2018	**5**	In Wireshark2.6.0 2.4.0 to 2.4.6 and 2.2.0 to 2.2.14 the RRC dissector and other dissectors could crash. This was addressed in epan/proto.c by avoiding a NULL pointer dereference. **CVE-ID:CVE-2018-11359**	https://www.wireshark.org/security/wnpa-sec-2018-33.html https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=14703 https://code.wiresh	**A-Wir-Wires/18-06-18/120**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;							

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
				ark.org/review/gitweb?p=wireshark.git;a=commit;h=beaebe91b14564fb9f86f0726bab09927872721b	
NA	22-05-2018	**5**	In Wireshark2.6.0 the IEEE 1905.1a dissector could crash. This was addressed in epan/dissectors/packet-ieee1905.c by making a certain correction to string handling. **CVE-ID:CVE-2018-11354**	https://www.wireshark.org/security/wnpa-sec-2018-26.html https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=14647 https://code.wireshark.org/review/gitweb?p=wireshark.git;a=commit;h=cb517a4a434387e74a2f75ebb106ee3c3893251c	**A-Wir-Wires/18-06-18/121**
Overflow	22-05-2018	**5**	In Wireshark2.6.0 2.4.0 to 2.4.6 and 2.2.0 to 2.2.14 the GSM A DTAP dissector could crash. This was addressed in epan/dissectors/packet-gsm_dtap.c by fixing an off-by-one error that caused a buffer overflow. **CVE-ID:CVE-2018-11360**	https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=14688https://code.wireshark.org/review/gitweb?p=wireshark.git;a=commit;h=a55b36c51f83a7b9680824e8ee3a6ce8429ab24bhttps://www.debian.org/security/2018/dsa-4217https://www.wireshark.org/security/wnpa-sec-2018-30.html	**A-Wir-Wires/18-06-18/122**
Overflow	22-05-2018	**5**	In Wireshark2.6.0 2.4.0 to 2.4.6 and 2.2.0 to 2.2.14 the LDSS dissector could crash. This was addressed in epan/dissectors/packet-ldss.c by	https://www.wireshark.org/security/wnpa-sec-2018-25.html https://www.debia	**A-Wir-Wires/18-06-18/123**

CV Scoring Scale (CVSS)	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			avoiding a buffer over-read upon encountering a missing '0' character. **CVE-ID:CVE-2018-11362**	n.org/security/2018/dsa-4217 https://lists.debian.org/debian-lts-announce/2018/05/msg00019.html https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=14615 https://code.wireshark.org/review/gitweb?p=wireshark.git;a=commit;h=f177008b04a530640de835ca878892e58b826d58	
Overflow	22-05-2018	**5**	In Wireshark2.6.0 the IEEE 802.11 protocol dissector could crash. This was addressed in epan/crypt/dot11decrypt.c by avoiding a buffer overflow during FTE processing in Dot11DecryptTDLSDeriveKey. **CVE-ID:CVE-2018-11361**	https://www.wireshark.org/security/wnpa-sec-2018-32.html https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=14686 https://code.wireshark.org/review/gitweb?p=wireshark.git;a=commit;h=1b52f9929238ce3948ec924ae4f9456b5e9df558	**A-Wir-Wires/18-06-18/124**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
Overflow	22-05-2018	**5**	In Wireshark2.6.0 the RTCP dissector could crash. This was addressed in epan/dissectors/packet-rtcp.c by avoiding a buffer overflow for packet status chunks. **CVE-ID:CVE-2018-11355**	https://www.wireshark.org/security/wnpa-sec-2018-27.html https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=14673 https://code.wireshark.org/review/gitweb?p=wireshark.git;a=commit;h=99d27a5fd2c540f837154aca3b3647f5ccfa0c33	**A-Wir-Wires/18-06-18/125**
ApplicationOperating System (ApplicationOS)					
CanonicalDebianImagemagick					
Debian LinuxImagemagickUbuntu Linux					
DoS	18-05-2018	**7.1**	In ImageMagick 7.0.7-16 Q16 x86_64 2017-12-22 an infinite loop vulnerability was found in the function ReadMIFFImage in coders/miff.c which allows attackers to cause a denial of service (CPU exhaustion) via a crafted MIFF image file. **CVE-ID:CVE-2017-18271**	https://github.com/ImageMagick/ImageMagick/issues/911 https://lists.debian.org/debian-lts-announce/2018/05/msg00012.html https://usn.ubuntu.com/3681-1/	**A-Can-Debia/18-06-18/126**
DoS	18-05-2018	**7.1**	In ImageMagick 7.0.7-16 Q16 x86_64 2017-12-22 an infinite loop vulnerability was found in the function ReadTXTImage in coders/txt.c which allows attackers to cause a denial of service (CPU exhaustion) via a crafted image file that is mishandled in a GetImageIndexInList call. **CVE-ID:CVE-2017-18273**	https://github.com/ImageMagick/ImageMagick/issues/910 https://usn.ubuntu.com/3681-1/ https://lists.debian.org/debian-lts-announce/2018/05/msg00012.html	**A-Can-Debia/18-06-18/127**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
Operatingt System (OS)					
Microsoft					
Windows 10Windows 7Windows 8.1Windows Rt 8.1Windows Server 2008Windows Server 2012Windows Server 2016					
Overflow Memory Corruption	14-06-2018	**7.6**	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory aka "Media Foundation Memory Corruption Vulnerability." This affects Windows 7 Windows Server 2012 R2 Windows RT 8.1 Windows Server 2012 Windows 8.1 Windows Server 2016 Windows Server 2008 R2 Windows 10 Windows 10 Servers. **CVE-ID:CVE-2018-8251**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8251	**O-Mic-Windo/18-06-18/128**
Windows 10Windows Server 2016					
NA	14-06-2018	**7.2**	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory aka "Win32k Elevation of Privilege Vulnerability." This affects Windows 10 Windows 10 Servers. **CVE-ID:CVE-2018-8233**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8233	**O-Mic-Windo/18-06-18/129**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;