



National Critical Information Infrastructure Protection Centre

CVE Report

CV Scoring Scale : 3-10

1 Sep -30 Sep 2018

Vol. 05 No.18

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/ Patch	NCIIPC ID
Application					
Easycms					
<i>Easycms</i>					
XSS	2018-09-10	3.5	EasyCMS 1.5 allows XSS via the index.php?s=/admin/fields/update/na vTabId/listfields/callbackType/closeC urrent content field. CVE ID : CVE-2018-16773	https://github.com/teameasy/EasyCMS/issues/6	A-EAS-EASYC-11018/1
Hongcms Project					
<i>Hongcms</i>					
Dir. Trav.	2018-09-10	6.4	HongCMS 3.0.0 allows arbitrary file deletion via a ../ in the file parameter to admin/index.php/ language /ajax?action=delete. CVE ID : CVE-2018-16774	https://github.com/Neke/HongCMS/issues/6	A-HON-HONGC-11018/2
Hoosk					
<i>Hoosk</i>					
XSS	2018-09-10	3.5	Hoosk v1.7.0 allows XSS via the Navigation Title of a new page entered at admin/pages/new. CVE ID : CVE-2018-16772	https://github.com/havok89/Hoosk/issues/47	A-HOO-HOOSK-11018/3
Exec Code	2018-09-10	7.5	Hoosk v1.7.0 allows PHP code execution via a SiteUrl that is provided during installation and mishandled in config.php. CVE ID : CVE-2018-16771	https://github.com/havok89/Hoosk/issues/46	A-HOO-HOOSK-11018/4
IBM					
<i>Campaign</i>					
Exec Code	2018-09-07	3.5	IBM Campaign 9.1, 9.1.2, and 10 is vulnerable to HTML injection. A remote attacker could inject malicious HTML code, which when viewed, would be executed in the victim's Web browser within the security context of the hosting site. IBM X-Force ID: 121153. CVE ID : CVE-2017-1115	https://www.ibm.com/support/docview.wss?uid=ibm10729769	A-IBM-CAMPA-11018/5
XSS	2018-09-07	3.5	IBM Campaign 9.1, 9.1.2, and 10 is vulnerable to cross-site scripting. This vulnerability allows users to embed	https://www.ibm.com/support/doc	A-IBM-CAMPA-11018/6

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	CVSS	Description & CVE ID	Reference/ Patch	NCIIPC ID			
			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: 121152. CVE ID : CVE-2017-1114	view.wss?uid=ibm10729773				
Security Identity Governance And Intelligence								
+Info	2018-09-07	5	IBM Security Identity Governance and Intelligence 5.2.3.2 and 5.2.4 could allow an attacker to obtain sensitive information due to missing authentication in IGI for the survey application. IBM X-Force ID: 148601. CVE ID : CVE-2018-1757	http://www.ibm.com/support/docview.wss?uid=ibm10728883	A-IBM-SECUR-11018/7			
Sql	2018-09-07	5	IBM Security Identity Governance and Intelligence 5.2.3.2 and 5.2.4 is vulnerable to SQL injection. A remote attacker could send specially-crafted SQL statements, which could allow the attacker to view, information in the back-end database. IBM X-Force ID: 148599. CVE ID : CVE-2018-1756	http://www.ibm.com/support/docview.wss?uid=ibm10728883	A-IBM-SECUR-11018/8			
WebSphere Application Server								
Execute Code	2018-09-07	7.5	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 could allow remote attackers to execute arbitrary Java code through the SOAP connector with a serialized object from untrusted sources. IBM X-Force ID: 143024. CVE ID : CVE-2018-1567	https://www.ibm.com/support/docview.wss?uid=swg22016254	A-IBM-WEBSP-11018/9			
Nordvpn								
Nordvpn								
Execute Code	2018-09-07	7.2	An exploitable code execution vulnerability exists in the connect functionality of NordVPN 6.14.28.0. A specially crafted configuration file can cause a privilege escalation, resulting in the execution of arbitrary commands with system privileges. CVE ID : CVE-2018-3952	NA	A-NOR-NORDV-11018/10			
Protonvpn								
Protonvpn								
Execute Code	2018-09-07	7.2	An exploitable code execution	NA	A-PRO-			
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	CVSS	Description & CVE ID	Reference/ Patch	NCIIPC ID
			vulnerability exists in the connect functionality of ProtonVPN VPN client 1.5.1. A specially crafted configuration file can cause a privilege escalation, resulting in the ability to execute arbitrary commands with the system's privileges. CVE ID : CVE-2018-4010		PROTO-11018/11
Weseek					
Growi					
XSS	2018-09-07	4.3	Cross-site scripting vulnerability in GROWI v.3.1.11 and earlier allows remote attackers to inject arbitrary web script or HTML via the modal for creating Wiki page. CVE ID : CVE-2018-0654	https://weseek.co.jp/security/2018/07/31/growi-prevent-xss/	A-WES-GROWI-11018/12
XSS	2018-09-07	4.3	Cross-site scripting vulnerability in GROWI v.3.1.11 and earlier allows remote attackers to inject arbitrary web script or HTML via Wiki page view. CVE ID : CVE-2018-0653	https://weseek.co.jp/security/2018/07/31/growi-prevent-xss/	A-WES-GROWI-11018/13
XSS	2018-09-07	3.5	Cross-site scripting vulnerability in GROWI v.3.1.11 and earlier allows remote authenticated attackers to inject arbitrary web script or HTML via the app settings section of admin page. CVE ID : CVE-2018-0655	https://weseek.co.jp/security/2018/07/31/growi-prevent-xss/	A-WES-GROWI-11018/14
XSS	2018-09-07	3.5	Cross-site scripting vulnerability in GROWI v.3.1.11 and earlier allows remote authenticated attackers to inject arbitrary web script or HTML via the UserGroup Management section of admin page. CVE ID : CVE-2018-0652	https://weseek.co.jp/security/2018/07/31/growi-prevent-xss/	A-WES-GROWI-11018/15

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;							