



National Critical Information Infrastructure Protection Centre

CVE Report

CV Scoring Scale : 3-10

15 Jun-15 Jul 2018

Vol. 05 No.13

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
Application					
Faststone					
Image Viewer					
Overflow	19-06-2018	6.8	FastStone Image Viewer 6.2 has a User Mode Read and Execute AV at 0x0057898e, triggered when the user opens a malformed JPEG file that is mishandled by FSViewer.exe. Attackers could exploit this issue for DoS (Access Violation) or possibly unspecified other impact. CVE-ID:CVE-2018-11707	https://github.com/MostafaSoliman/Security-Advisories/tree/master/CVE-2018-11707	A-Fas-Image/16-07-18/1
Overflow	19-06-2018	6.8	FastStone Image Viewer 6.2 has a User Mode Write AV at 0x00402d6a, triggered when the user opens a malformed JPEG file that is mishandled by FSViewer.exe. Attackers could exploit this issue for DoS (Access Violation) or possibly unspecified other impact. CVE-ID:CVE-2018-11703	https://github.com/MostafaSoliman/Security-Advisories/tree/master/CVE-2018-11703	A-Fas-Image/16-07-18/2
Overflow	19-06-2018	6.8	FastStone Image Viewer 6.2 has a User Mode Write AV at 0x00402d7d, triggered when the user opens a malformed JPEG file that is mishandled by FSViewer.exe. Attackers could exploit this issue for DoS (Access Violation) or possibly unspecified other impact. CVE-ID:CVE-2018-11704	https://github.com/MostafaSoliman/Security-Advisories/tree/master/CVE-2018-11704	A-Fas-Image/16-07-18/3
Overflow	19-06-2018	6.8	FastStone Image Viewer 6.2 has a User Mode Write AV at 0x00578cb3, triggered when the user opens a malformed	https://github.com/MostafaSoliman/Security-Advisories/tree/m	A-Fas-Image/16-07-18/4

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	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			JPEG file that is mishandled by FSViewer.exe. Attackers could exploit this issue for DoS (Access Violation) or possibly unspecified other impact. CVE-ID:CVE-2018-11702	aster/CVE-2018-11702	
Overflow	19-06-2018	6.8	FastStone Image Viewer 6.2 has a User Mode Write AV at 0x00578cc4, triggered when the user opens a malformed JPEG file that is mishandled by FSViewer.exe. Attackers could exploit this issue for DoS (Access Violation) or possibly unspecified other impact. CVE-ID:CVE-2018-11705	https://github.com/MostafaSoliman/Security-Advisories/tree/master/CVE-2018-11705	A-Fas-Image/16-07-18/5
Overflow	19-06-2018	6.8	FastStone Image Viewer 6.2 has a User Mode Write AV at 0x00578dd8, triggered when the user opens a malformed JPEG file that is mishandled by FSViewer.exe. Attackers could exploit this issue for DoS (Access Violation) or possibly unspecified other impact. CVE-ID:CVE-2018-11706	https://github.com/MostafaSoliman/Security-Advisories/tree/master/CVE-2018-11706	A-Fas-Image/16-07-18/6
Overflow	19-06-2018	6.8	FastStone Image Viewer 6.2 has a User Mode Write AV at 0x005cb509, triggered when the user opens a malformed JPEG file that is mishandled by FSViewer.exe. Attackers could exploit this issue for DoS (Access Violation) or possibly unspecified other impact. CVE-ID:CVE-2018-11701	https://github.com/MostafaSoliman/Security-Advisories/tree/master/CVE-2018-11701	A-Fas-Image/16-07-18/7

Perfsonar

Monitoring And Debugging Dashboard

Gain Information	18-06-2018	5	An issue was discovered in perfSONAR Monitoring and Debugging Dashboard (MaDDash) 2.0.2. A direct	https://www.exploit-db.com/exploits/44910/	A-Per-Monit/16-07-18/8
------------------	------------	---	---	---	-------------------------------

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
			request to /etc/ provides a directory listing. CVE-ID:CVE-2018-12523	https://pastebin.com/eA5tGKf0	
Gain Information	18-06-2018	5	An issue was discovered in perfSONAR Monitoring and Debugging Dashboard (MaDDash) 2.0.2. A direct request to /images/ provides a directory listing. CVE-ID:CVE-2018-12525	https://www.exploit-db.com/exploits/44910/ , https://pastebin.com/eA5tGKf0	A-Per-Monit/16-07-18/9
Gain Information	18-06-2018	5	An issue was discovered in perfSONAR Monitoring and Debugging Dashboard (MaDDash) 2.0.2. A direct request to /lib/ provides a directory listing. CVE-ID:CVE-2018-12524	https://www.exploit-db.com/exploits/44910/ , https://pastebin.com/eA5tGKf0	A-Per-Monit/16-07-18/10
Gain Information	18-06-2018	5	An issue was discovered in perfSONAR Monitoring and Debugging Dashboard (MaDDash) 2.0.2. A direct request to /style/ provides a directory listing. CVE-ID:CVE-2018-12522	https://www.exploit-db.com/exploits/44910/ , https://pastebin.com/eA5tGKf0	A-Per-Monit/16-07-18/11

Servviziotoken Project

Servviziotoken

Overflow	09-07-2018	5	The mintToken function of a smart contract implementation for SERVIZIOToken, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13723	https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md , https://github.com/BlockChainsSecurity/EtherTokens/tree/master/SERVIZIOToken	A-Ser-Servv/16-07-18/12
----------	------------	---	---	--	--------------------------------

Hardware

ARM,Intel

Atom C,Atom E,Atom X3,Atom Z,Celeron J,Celeron N,Core I3,Core I5,Core I7,Core M,Core M3,Core

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
M5,Core M7,Cortex-a,Cortex-r,Pentium J,Pentium N,Xeon,Xeon Bronze,Xeon E3					
Overflow Gain Information	10-07-2018	4.7	Systems with microprocessors utilizing speculative execution and branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a speculative buffer overflow and side-channel analysis. CVE-ID:CVE-2018-3693	https://www.suse.com/support/kb/doc/?id=7023075, https://thehackernews.com/2018/07/intel-spectre-vulnerability.html, https://01.org/security/advisories/intel-oss-10002	H-ARM-Atom/16-07-18/13
Core I3,Core I5,Core I7,Core M,Core M3,Core M5,Core M7,Cortex-a					
Gain Information	21-06-2018	4.7	System software utilizing Lazy FP state restore technique on systems using Intel Core-based microprocessors may potentially allow a local process to infer data from another process through a speculative execution side channel. CVE-ID:CVE-2018-3665	https://www.synology.com/support/security/Synology_S18_31, https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00145.html, https://usn.ubuntu.com/3698-2/, https://www.debian.org/security/2018/dsa-4232, https://usn.ubuntu.com/3698-1/, https://support.citrix.com/article/CTX235745, https://usn.ubuntu.com/3696-1/, https://usn.ubuntu.com/3696-1/,	H-ARM-Core/16-07-18/14

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
				u.com/3696-2/ , https://security.FreeBSD.org/advisories/FreeBSD-SA-18:07.lazyfpu.asc , https://access.redhat.com/errata/RHSA-2018:1944 , https://access.redhat.com/errata/RHSA-2018:2165 , https://access.redhat.com/errata/RHSA-2018:2164 , https://access.redhat.com/errata/RHSA-2018:1852	

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;							