Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application					
5none					
nonecms					
Cross-Site Request Forgery (CSRF)	23-09-2019	5.8	NoneCMS v1.3 has CSRF in public/index.php/admin/admin/dele.html, as demonstrated by deleting the admin user. **CVE ID : CVE-2019-16721**	N/A	A-5NO-NONE-141019/1
Advantech					
Webaccess/hmi_designer					
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-09-2019	5	In Advantech WebAccess/HMI Designer 2.1.9.31, Data from a Faulting Address controls Code Flow starting at PM_V3!CTagInfoThreadBase::GetNICInfo+0x0000000000512918. **CVE ID : CVE-2019-16899**	N/A	A-ADV-WEBA-141019/2
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-09-2019	5	Advantech WebAccess/HMI Designer 2.1.9.31 has a User Mode Write AV starting at MSVCR90!memcpy+0x000000000000015c. **CVE ID : CVE-2019-16900**	N/A	A-ADV-WEBA-141019/3
Improper Handling of Exceptional Conditions	25-09-2019	5	Advantech WebAccess/HMI Designer 2.1.9.31 has Exception Handler Chain corruption starting at Unknown Symbol @	N/A	A-ADV-WEBA-141019/4

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			0x0000000000000000 called from ntdll!RtlRaiseStatus+0x0000000000000000b4. **CVE ID : CVE-2019-16901**		
webaccess					
Incorrect Authorization	18-09-2019	9	In WebAccess, versions 8.4.1 and prior, an improper authorization vulnerability may allow an attacker to disclose sensitive information, cause improper control of generation of code, which may allow remote code execution or cause a system crash. **CVE ID : CVE-2019-13550**	N/A	A-ADV-WEBA-141019/5
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-09-2019	6.5	In WebAccess versions 8.4.1 and prior, multiple command injection vulnerabilities are caused by a lack of proper validation of user-supplied data and may allow arbitrary file deletion and remote code execution. **CVE ID : CVE-2019-13552**	N/A	A-ADV-WEBA-141019/6
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-09-2019	6.5	In WebAccess versions 8.4.1 and prior, multiple stack-based buffer overflow vulnerabilities are caused by a lack of proper validation of the length of user-supplied data. Exploitation of these vulnerabilities may allow remote code execution. **CVE ID : CVE-2019-13556**	N/A	A-ADV-WEBA-141019/7
Improper Control of	18-09-2019	9	In WebAccess versions 8.4.1 and prior, an exploit	N/A	A-ADV-WEBA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation of Code ('Code Injection')			executed over the network may cause improper control of generation of code, which may allow remote code execution, data exfiltration, or cause a system crash. **CVE ID : CVE-2019-13558**		141019/8
Apache					
tapestry					
Deserialization of Untrusted Data	16-09-2019	7.5	Manipulating classpath asset file URLs, an attacker could guess the path to a known file in the classpath and have it downloaded. If the attacker found the file with the value of the tapestry.hmac-passphrase configuration symbol, most probably the webapp's AppModule class, the value of this symbol could be used to craft a Java deserialization attack, thus running malicious injected Java code. The vector would be the t:formdata parameter from the Form component. **CVE ID : CVE-2019-0195**	N/A	A-APA-TAPE-141019/9
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-09-2019	5	Tapestry processes assets `/assets/ctx` using classes chain `StaticFilesFilter -> AssetDispatcher -> ContextResource`, which doesn't filter the character `\`, so attacker can perform a path traversal attack to read any files on Windows platform. **CVE ID : CVE-2019-0207**	N/A	A-APA-TAPE-141019/10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	16-09-2019	6.8	The code which checks HMAC in form submissions used String.equals() for comparisons, which results in a timing side channel for the comparison of the HMAC signatures. This could lead to remote code execution if an attacker is able to determine the correct signature for their payload. The comparison should be done with a constant time algorithm instead. **CVE ID : CVE-2019-10071**	N/A	A-APA-TAPE-141019/11
subversion					
Improper Input Validation	26-09-2019	5	In Apache Subversion versions up to and including 1.9.10, 1.10.4, 1.12.0, Subversion's svnserve server process may exit when a client sends certain sequences of protocol commands. This can lead to disruption for users of the server. **CVE ID : CVE-2019-0203**	N/A	A-APA-SUBV-141019/12
http_server					
Use After Free	26-09-2019	6.4	In Apache HTTP Server 2.4.18-2.4.39, using fuzzed network input, the http/2 session handling could be made to read memory after being freed, during connection shutdown. **CVE ID : CVE-2019-10082**	N/A	A-APA-HTTP-141019/13
Improper Neutralization of Input	26-09-2019	4.3	In Apache HTTP Server 2.4.0-2.4.39, a limited cross-site scripting issue was	N/A	A-APA-HTTP-141019/14

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			reported affecting the mod_proxy error page. An attacker could cause the link on the error page to be malformed and instead point to a page of their choice. This would only be exploitable where a server was set up with proxying enabled but was misconfigured in such a way that the Proxy Error page was displayed. **CVE ID : CVE-2019-10092**		
NULL Pointer Dereference	26-09-2019	6	In Apache HTTP Server 2.4.32-2.4.39, when mod_remoteip was configured to use a trusted intermediary proxy server using the "PROXY" protocol, a specially crafted PROXY header could trigger a stack buffer overflow or NULL pointer deference. This vulnerability could only be triggered by a trusted proxy and not by untrusted HTTP clients. **CVE ID : CVE-2019-10097**	N/A	A-APA-HTTP-141019/15
URL Redirection to Untrusted Site ('Open Redirect')	25-09-2019	5.8	In Apache HTTP server 2.4.0 to 2.4.39, Redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an unexpected URL within the request URL. **CVE ID : CVE-2019-10098**	N/A	A-APA-HTTP-141019/16

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
jspwiki					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-09-2019	4.3	On Apache JSPWiki, up to version 2.11.0.M4, a carefully crafted plugin link invocation could trigger an XSS vulnerability on Apache JSPWiki, related to the Page Revision History, which could allow the attacker to execute javascript in the victim's browser and get some sensitive information about the victim. **CVE ID : CVE-2019-10087**	N/A	A-APA-JSPW-141019/17
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-09-2019	4.3	On Apache JSPWiki, up to version 2.11.0.M4, a carefully crafted plugin link invocation could trigger an XSS vulnerability on Apache JSPWiki, related to the WYSIWYG editor, which could allow the attacker to execute javascript in the victim's browser and get some sensitive information about the victim. **CVE ID : CVE-2019-10089**	N/A	A-APA-JSPW-141019/18
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-09-2019	4.3	On Apache JSPWiki, up to version 2.11.0.M4, a carefully crafted plugin link invocation could trigger an XSS vulnerability on Apache JSPWiki, related to the plain editor, which could allow the attacker to execute javascript in the victim's browser and get some sensitive information about the victim.	N/A	A-APA-JSPW-141019/19

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10090		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-09-2019	4.3	On Apache JSPWiki, up to version 2.11.0.M4, a carefully crafted plugin link invocation could trigger an XSS vulnerability on Apache JSPWiki, related to InfoContent.jsp, which could allow the attacker to execute javascript in the victim's browser and get some sensitive information about the victim. **CVE ID : CVE-2019-12404**	N/A	A-APA-JSPW-141019/20
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-09-2019	4.3	On Apache JSPWiki, up to version 2.11.0.M4, a carefully crafted plugin link invocation could trigger an XSS vulnerability on Apache JSPWiki, related to the remember parameter on some of the JSPs, which could allow the attacker to execute javascript in the victim's browser and get some sensitive information about the victim. **CVE ID : CVE-2019-12407**	N/A	A-APA-JSPW-141019/21
Apereo					
central_authentication_service					
Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)	23-09-2019	5.5	Multiple classes used within Apereo CAS before release 6.1.0-RC5 makes use of apache commons-lang3 RandomStringUtils for token and ID generation which makes them predictable due to RandomStringUtils PRNG's algorithm not being	N/A	A-APE-CENT-141019/22

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			cryptographically strong. **CVE ID : CVE-2019-10754**		
aspose					
aspose.pdf_for_c++					
Use After Free	18-09-2019	7.5	An uninitialized memory access vulnerability exists in the way Aspose.PDF 19.2 for C++ handles invalid parent object pointers. A specially crafted PDF can cause a read and write from uninitialized memory, resulting in memory corruption and possibly arbitrary code execution. To trigger this vulnerability, a specifically crafted PDF document needs to be processed by the target application. **CVE ID : CVE-2019-5067**	https://www.talosintelligence.com/vulnerability_reports/TALOS-2019-0856	A-ASP-ASPO-141019/23
Use After Free	18-09-2019	6.5	An exploitable Use-After-Free vulnerability exists in the way FunctionType 0 PDF elements are processed in Aspose.PDF 19.2 for C++. A specially crafted PDF can cause a dangling heap pointer, resulting in a use-after-free. An attacker can send a malicious PDF to trigger this vulnerability. **CVE ID : CVE-2019-5042**	https://www.talosintelligence.com/vulnerability_reports/TALOS-2019-0809	A-ASP-ASPO-141019/24
Use After Free	18-09-2019	7.5	An exploitable use-after-free vulnerability exists in the way LZW-compressed streams are processed in Aspose.PDF 19.2 for C++. A specially crafted PDF can cause a dangling heap	https://www.talosintelligence.com/vulnerability_reports/TALOS-2019-	A-ASP-ASPO-141019/25

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			pointer, resulting in a use-after-free condition. To trigger this vulnerability, a specifically crafted PDF document needs to be processed by the target application. **CVE ID : CVE-2019-5066**	0855	
Atlassian					
jira					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	19-09-2019	9	The Jira Importers Plugin in Atlassian Jira Server and Data Cente from version with 7.0.10 before 7.6.16, from 7.7.0 before 7.13.8, from 8.1.0 before 8.1.3, from 8.2.0 before 8.2.5, from 8.3.0 before 8.3.4 and from 8.4.0 before 8.4.1 allows remote attackers with Administrator permissions to gain remote code execution via a template injection vulnerability through the use of a crafted PUT request. **CVE ID : CVE-2019-15001**	N/A	A-ATL-JIRA-141019/26
bitbucket					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	19-09-2019	6.8	The commit diff rest endpoint in Bitbucket Server and Data Center before 5.16.10 (the fixed version for 5.16.x), from 6.0.0 before 6.0.10 (the fixed version for 6.0.x), from 6.1.0 before 6.1.8 (the fixed version for 6.1.x), from 6.2.0 before 6.2.6 (the fixed version for 6.2.x), from 6.3.0 before 6.3.5 (the fixed version for	N/A	A-ATL-BITB-141019/27

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			6.3.x), from 6.4.0 before 6.4.3 (the fixed version for 6.4.x), and from 6.5.0 before 6.5.2 (the fixed version for 6.5.x) allows remote attackers who have permission to access a repository, if public access is enabled for a project or repository then attackers are able to exploit this issue anonymously, to read the contents of arbitrary files on the system and execute commands via injecting additional arguments into git commands. **CVE ID : CVE-2019-15000**		
jira_service_desk_server					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	19-09-2019	4.3	The Customer Context Filter in Atlassian Jira Service Desk Server and Jira Service Desk Data Center before version 3.9.16, from version 3.10.0 before version 3.16.8, from version 4.0.0 before version 4.1.3, from version 4.2.0 before version 4.2.5, from version 4.3.0 before version 4.3.4, and version 4.4.0 allows remote attackers with portal access to view arbitrary issues in Jira Service Desk projects via a path traversal vulnerability. Note that when the 'Anyone can email the service desk or raise a request in the portal' setting is enabled, an attacker can grant	N/A	A-ATL-JIRA-141019/28

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			themselves portal access, allowing them to exploit the vulnerability. **CVE ID : CVE-2019-14994**		
axiosys					
bento4					
NULL Pointer Dereference	16-09-2019	4.3	Bento4 1.5.1-628 has a NULL pointer dereference in AP4_ByteStream::ReadUI32 in Core/Ap4ByteStream.cpp when called from the AP4_TrunAtom class. **CVE ID : CVE-2019-16349**	N/A	A-AXI-BENT-141019/29
beego					
beego					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	1.9	The File Session Manager in Beego 1.10.0 allows local users to read session files because there is a race condition involving file creation within a directory with weak permissions. **CVE ID : CVE-2019-16354**	N/A	A-BEE-BEEG-141019/30
Incorrect Default Permissions	16-09-2019	2.1	The File Session Manager in Beego 1.10.0 allows local users to read session files because of weak permissions for individual files. **CVE ID : CVE-2019-16355**	N/A	A-BEE-BEEG-141019/31
Bluestacks					
bluestacks					
Information Exposure	24-09-2019	4.9	An issue was discovered in BlueStacks 4.110 and below on macOS and on 4.120 and below on Windows. BlueStacks employs Android	https://support.bluestacks.com/hc/en-us/articles/	A-BLU-BLUE-141019/32

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			running in a virtual machine (VM) to enable Android apps to run on Windows or MacOS. Bug is in a local arbitrary file read through a system service call. The impacted method runs with System admin privilege and if given the file name as parameter returns you the content of file. A malicious app using the affected method can then read the content of any system file which it is not authorized to read **CVE ID : CVE-2019-14220**	360033484132-BlueStacks-fails-to-restrict-access-permissions	
Cacti					
cacti					
Authorization Bypass Through User-Controlled Key	23-09-2019	4	In Cacti through 1.2.6, authenticated users may bypass authorization checks (for viewing a graph) via a direct graph_json.php request with a modified local_graph_id parameter. **CVE ID : CVE-2019-16723**	N/A	A-CAC-CACT-141019/33
Centreon					
centreon					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-09-2019	7.5	SQL injection vulnerabilities in Centreon through 19.04 allow attacks via the svc_id parameter in include/monitoring/status/Services/xml/makeXMLForOneService.php. **CVE ID : CVE-2019-16194**	N/A	A-CEN-CENT-141019/34

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
checklist					
checklist					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-09-2019	4.3	An XSS issue was discovered in the checklist plugin before 1.1.9 for WordPress. The fill parameter is not correctly filtered in the checklist-icon.php file, and it is possible to inject JavaScript code. **CVE ID : CVE-2019-16525**	N/A	A-CHE-CHEC-141019/35
cloudfoundry					
cf-deployment					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	23-09-2019	5.5	Cloud Foundry NFS Volume Service, 1.7.x versions prior to 1.7.11 and 2.x versions prior to 2.3.0, is vulnerable to LDAP injection. A remote authenticated malicious space developer can potentially inject LDAP filters via service instance creation, facilitating the malicious space developer to deny service or perform a dictionary attack. **CVE ID : CVE-2019-11277**	https://www.cloudfoundry.org/blog/cve-2019-11277	A-CLO-CF-D-141019/36
code42					
code42					
Unrestricted Upload of File with Dangerous Type	17-09-2019	7.5	In Code42 Enterprise 6.7.5 and earlier, 6.8.4 through 6.8.8, and 7.0.0 a vulnerability has been identified that may allow arbitrary files to be uploaded to Code42 servers and executed. This vulnerability could allow an attacker to	N/A	A-COD-CODE-141019/37

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			create directories and save files on Code42 servers, which could potentially lead to code execution. **CVE ID : CVE-2019-15131**		
Codesys					
control_for_beaglebone					
Incorrect Permission Assignment for Critical Resource	17-09-2019	6.5	An issue was discovered in 3S-Smart CODESYS V3 through 3.5.12.30. A user with low privileges can take full control over the runtime. **CVE ID : CVE-2019-9008**	N/A	A-COD-CONT-141019/38
control_for_empc-a/imx6					
Incorrect Permission Assignment for Critical Resource	17-09-2019	6.5	An issue was discovered in 3S-Smart CODESYS V3 through 3.5.12.30. A user with low privileges can take full control over the runtime. **CVE ID : CVE-2019-9008**	N/A	A-COD-CONT-141019/39
control_for_iot2000					
Incorrect Permission Assignment for Critical Resource	17-09-2019	6.5	An issue was discovered in 3S-Smart CODESYS V3 through 3.5.12.30. A user with low privileges can take full control over the runtime. **CVE ID : CVE-2019-9008**	N/A	A-COD-CONT-141019/40
control_for_pfc100					
Incorrect Permission Assignment for Critical Resource	17-09-2019	6.5	An issue was discovered in 3S-Smart CODESYS V3 through 3.5.12.30. A user with low privileges can take full control over the runtime. **CVE ID : CVE-2019-9008**	N/A	A-COD-CONT-141019/41
control_for_pfc200					
Incorrect	17-09-2019	6.5	An issue was discovered in	N/A	A-COD-CONT-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Permission Assignment for Critical Resource			3S-Smart CODESYS V3 through 3.5.12.30. A user with low privileges can take full control over the runtime. **CVE ID : CVE-2019-9008**		141019/42
control_for_raspberry_pi					
Incorrect Permission Assignment for Critical Resource	17-09-2019	6.5	An issue was discovered in 3S-Smart CODESYS V3 through 3.5.12.30. A user with low privileges can take full control over the runtime. **CVE ID : CVE-2019-9008**	N/A	A-COD-CONT-141019/43
codesys					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-09-2019	6.8	3S-Smart Software Solutions GmbH CODESYS V3 Library Manager, all versions prior to 3.5.15.0, allows the system to display active library content without checking its validity, which may allow the contents of manipulated libraries to be displayed or executed. The issue also exists for source libraries, but 3S-Smart Software Solutions GmbH strongly recommends distributing compiled libraries only. **CVE ID : CVE-2019-13538**	N/A	A-COD-CODE-141019/44
cure53					
dompurify					
Improper Neutralization of Input During Web Page Generation	24-09-2019	4.3	DOMPurify before 2.0.1 allows XSS because of innerHTML mutation XSS (mXSS) for an SVG element or a MATH element, as demonstrated by Chrome	N/A	A-CUR-DOMP-141019/45

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			and Safari. **CVE ID : CVE-2019-16728**		
devise_token_auth_project					
devise_token_auth					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-09-2019	4.3	An issue was discovered in Devise Token Auth through 1.1.2. The omniauth failure endpoint is vulnerable to Reflected Cross Site Scripting (XSS) through the message parameter. Unauthenticated attackers can craft a URL that executes a malicious JavaScript payload in the victim's browser. This affects the fallback_render method in the omniauth callbacks controller. **CVE ID : CVE-2019-16751**	N/A	A-DEV-DEVI-141019/46
digimute					
ogma_cms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-09-2019	3.5	Ogma CMS 0.5 has XSS via creation of a new blog. **CVE ID : CVE-2019-16661**	N/A	A-DIG-OGMA-141019/47
dnnsoftware					
dotnetnuke					
Improper Neutralization of Input During Web Page Generation	26-09-2019	4.3	Stored Cross-Site Scripting in DotNetNuke (DNN) Version before 9.4.0 allows remote attackers to store and embed the malicious script into the admin	N/A	A-DNN-DOTN-141019/48

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			notification page. The exploit could be used to perfom any action with admin privileges such as managing content, adding users, uploading backdoors to the server, etc. Successful exploitation occurs when an admin user visits a notification page with stored cross-site scripting. **CVE ID : CVE-2019-12562**		
Docker					
docker					
Incorrect Authorization	25-09-2019	5	runc through 1.0.0-rc8, as used in Docker through 19.03.2-ce and other products, allows AppArmor restriction bypass because libcontainer/rootfs_linux.go incorrectly checks mount targets, and thus a malicious Docker image can mount over a /proc directory. **CVE ID : CVE-2019-16884**	N/A	A-DOC-DOCK-141019/49
Dolibarr					
dolibarr					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-09-2019	4.3	In htdocs/societe/card.php in Dolibarr 10.0.1, the value of the User-Agent HTTP header is copied into the HTML document as plain text between tags, leading to XSS. **CVE ID : CVE-2019-16197**	N/A	A-DOL-DOLI-141019/50
Improper Neutralization of Input	27-09-2019	3.5	Dolibarr 9.0.5 has stored XSS in a User Note section to note.php. A user with no	N/A	A-DOL-DOLI-141019/51

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			privileges can inject script to attack the admin. **CVE ID : CVE-2019-16686**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-09-2019	3.5	Dolibarr 9.0.5 has stored XSS in a User Profile in a Signature section to card.php. A user with the "Create/modify other users, groups and permissions" privilege can inject script and can also achieve privilege escalation. **CVE ID : CVE-2019-16687**	N/A	A-DOL-DOLI-141019/52
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-09-2019	3.5	Dolibarr 9.0.5 has stored XSS in an Email Template section to mails_templates.php. A user with no privileges can inject script to attack the admin. (This stored XSS can affect all types of user privilege from Admin to users with no permissions.) **CVE ID : CVE-2019-16688**	N/A	A-DOL-DOLI-141019/53
e2fsprogs_project					
e2fsprogs					
Out-of-bounds Write	24-09-2019	4.6	An exploitable code execution vulnerability exists in the quota file functionality of E2fsprogs 1.45.3. A specially crafted ext4 partition can cause an out-of-bounds write on the heap, resulting in code execution. An attacker can corrupt a partition to trigger this vulnerability.	N/A	A-E2F-E2FS-141019/54

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-5094		
Eclipse					
mosquitto					
Use After Free	18-09-2019	5.5	If an MQTT v5 client connects to Eclipse Mosquitto versions 1.6.0 to 1.6.4 inclusive, sets a last will and testament, sets a will delay interval, sets a session expiry interval, and the will delay interval is set longer than the session expiry interval, then a use after free error occurs, which has the potential to cause a crash in some situations. **CVE ID : CVE-2019-11778**	https://bugs.eclipse.org/bugs/show_bug.cgi?id=551162	A-ECL-MOSQ-141019/55
Improper Check for Unusual or Exceptional Conditions	19-09-2019	4	In Eclipse Mosquitto 1.5.0 to 1.6.5 inclusive, if a malicious MQTT client sends a SUBSCRIBE packet containing a topic that consists of approximately 65400 or more '/' characters, i.e. the topic hierarchy separator, then a stack overflow will occur. **CVE ID : CVE-2019-11779**	N/A	A-ECL-MOSQ-141019/56
egpp					
sistema_integrado_de_gestion_academica					
Improper Neutralization of Special Elements used in an SQL Command	16-09-2019	7.5	In Escuela de Gestion Publica Plurinacional (EGPP) Sistema Integrado de Gestion Academica (GESAC) v1, the username parameter of the authentication form is vulnerable to SQL injection,	N/A	A-EGP-SIST-141019/57

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			allowing attackers to access the database. **CVE ID : CVE-2019-16264**		
Embedthis					
goahead					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-09-2019	5	An issue was discovered in Embedthis GoAhead 2.5.0. Certain pages (such as goform/login and config/log_off_page.htm) create links containing a hostname obtained from an arbitrary HTTP Host header sent by an attacker. This could potentially be used in a phishing attack. **CVE ID : CVE-2019-16645**	N/A	A-EMB-GOAH-141019/58
emlog					
emlog					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	25-09-2019	7.5	emlog through 6.0.0beta has an arbitrary file deletion vulnerability via an admin/data.php?action=dell_all_bak request with directory traversal sequences in the bak[] parameter. **CVE ID : CVE-2019-16868**	N/A	A-EML-EMLO-141019/59
F5					
big-ip_access_policy_manager					
Information Exposure Through Discrepancy	25-09-2019	5	In BIG-IP 15.0.0, 14.1.0-14.1.0.6, 14.0.0-14.0.0.5, 13.0.0-13.1.1.5, 12.1.0-12.1.4.1, 11.5.1-11.6.4, BIG-IQ 7.0.0, 6.0.0-6.1.0,5.2.0-5.4.0, iWorkflow 2.3.0, and Enterprise Manager 3.1.1,	N/A	A-F5-BIG--141019/60

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the Configuration utility login page may not follow best security practices when handling a malicious request. **CVE ID : CVE-2019-6651**		
Improper Input Validation	25-09-2019	3.3	On versions 14.0.0-14.1.2, 13.0.0-13.1.3, 12.1.0-12.1.5, and 11.5.1-11.6.5, the BIG-IP system fails to perform Martian Address Filtering (As defined in RFC 1812 section 5.3.7) on the control plane (management interface). This may allow attackers on an adjacent system to force BIG-IP into processing packets with spoofed source addresses. **CVE ID : CVE-2019-6654**	N/A	A-F5-BIG--141019/61
Information Exposure	25-09-2019	4.3	On versions 13.0.0-13.1.0.1, 12.1.0-12.1.4.1, 11.6.1-11.6.4, and 11.5.1-11.5.9, BIG-IP platforms where AVR, ASM, APM, PEM, AFM, and/or AAM is provisioned may leak sensitive data. **CVE ID : CVE-2019-6655**	N/A	A-F5-BIG--141019/62
big-ip_advanced_firewall_manager					
Information Exposure Through Discrepancy	25-09-2019	5	In BIG-IP 15.0.0, 14.1.0-14.1.0.6, 14.0.0-14.0.0.5, 13.0.0-13.1.1.5, 12.1.0-12.1.4.1, 11.5.1-11.6.4, BIG-IQ 7.0.0, 6.0.0-6.1.0,5.2.0-5.4.0, iWorkflow 2.3.0, and Enterprise Manager 3.1.1, the Configuration utility login page may not follow best security practices when	N/A	A-F5-BIG--141019/63

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			handling a malicious request. **CVE ID : CVE-2019-6651**		
Improper Input Validation	25-09-2019	3.3	On versions 14.0.0-14.1.2, 13.0.0-13.1.3, 12.1.0-12.1.5, and 11.5.1-11.6.5, the BIG-IP system fails to perform Martian Address Filtering (As defined in RFC 1812 section 5.3.7) on the control plane (management interface). This may allow attackers on an adjacent system to force BIG-IP into processing packets with spoofed source addresses. **CVE ID : CVE-2019-6654**	N/A	A-F5-BIG--141019/64
Information Exposure	25-09-2019	4.3	On versions 13.0.0-13.1.0.1, 12.1.0-12.1.4.1, 11.6.1-11.6.4, and 11.5.1-11.5.9, BIG-IP platforms where AVR, ASM, APM, PEM, AFM, and/or AAM is provisioned may leak sensitive data. **CVE ID : CVE-2019-6655**	N/A	A-F5-BIG--141019/65
big-ip_analytics					
Information Exposure Through Discrepancy	25-09-2019	5	In BIG-IP 15.0.0, 14.1.0-14.1.0.6, 14.0.0-14.0.0.5, 13.0.0-13.1.1.5, 12.1.0-12.1.4.1, 11.5.1-11.6.4, BIG-IQ 7.0.0, 6.0.0-6.1.0,5.2.0-5.4.0, iWorkflow 2.3.0, and Enterprise Manager 3.1.1, the Configuration utility login page may not follow best security practices when handling a malicious request.	N/A	A-F5-BIG--141019/66

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-6651		
Improper Input Validation	25-09-2019	3.3	On versions 14.0.0-14.1.2, 13.0.0-13.1.3, 12.1.0-12.1.5, and 11.5.1-11.6.5, the BIG-IP system fails to perform Martian Address Filtering (As defined in RFC 1812 section 5.3.7) on the control plane (management interface). This may allow attackers on an adjacent system to force BIG-IP into processing packets with spoofed source addresses. **CVE ID : CVE-2019-6654**	N/A	A-F5-BIG--141019/67
Information Exposure	25-09-2019	4.3	On versions 13.0.0-13.1.0.1, 12.1.0-12.1.4.1, 11.6.1-11.6.4, and 11.5.1-11.5.9, BIG-IP platforms where AVR, ASM, APM, PEM, AFM, and/or AAM is provisioned may leak sensitive data. **CVE ID : CVE-2019-6655**	N/A	A-F5-BIG--141019/68
big-ip_application_acceleration_manager					
Information Exposure Through Discrepancy	25-09-2019	5	In BIG-IP 15.0.0, 14.1.0-14.1.0.6, 14.0.0-14.0.0.5, 13.0.0-13.1.1.5, 12.1.0-12.1.4.1, 11.5.1-11.6.4, BIG-IQ 7.0.0, 6.0.0-6.1.0,5.2.0-5.4.0, iWorkflow 2.3.0, and Enterprise Manager 3.1.1, the Configuration utility login page may not follow best security practices when handling a malicious request. **CVE ID : CVE-2019-6651**	N/A	A-F5-BIG--141019/69
Improper Input	25-09-2019	3.3	On versions 14.0.0-14.1.2, 13.0.0-13.1.3, 12.1.0-12.1.5,	N/A	A-F5-BIG--

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			and 11.5.1-11.6.5, the BIG-IP system fails to perform Martian Address Filtering (As defined in RFC 1812 section 5.3.7) on the control plane (management interface). This may allow attackers on an adjacent system to force BIG-IP into processing packets with spoofed source addresses. **CVE ID : CVE-2019-6654**		141019/70
Information Exposure	25-09-2019	4.3	On versions 13.0.0-13.1.0.1, 12.1.0-12.1.4.1, 11.6.1-11.6.4, and 11.5.1-11.5.9, BIG-IP platforms where AVR, ASM, APM, PEM, AFM, and/or AAM is provisioned may leak sensitive data. **CVE ID : CVE-2019-6655**	N/A	A-F5-BIG--141019/71
big-ip_application_security_manager					
Information Exposure	20-09-2019	5.8	F5 BIG-IP ASM 15.0.0, 14.1.0-14.1.0.6, 14.0.0-14.0.0.5, 13.0.0-13.1.1.5, 12.1.0-12.1.4.1, 11.6.0-11.6.4, and 11.5.1-11.5.9 may expose sensitive information and allow the system configuration to be modified when using non-default settings. **CVE ID : CVE-2019-6650**	https://support.f5.com/csp/article/K04280042	A-F5-BIG--141019/72
Information Exposure Through Discrepancy	25-09-2019	5	In BIG-IP 15.0.0, 14.1.0-14.1.0.6, 14.0.0-14.0.0.5, 13.0.0-13.1.1.5, 12.1.0-12.1.4.1, 11.5.1-11.6.4, BIG-IQ 7.0.0, 6.0.0-6.1.0,5.2.0-5.4.0, iWorkflow 2.3.0, and Enterprise Manager 3.1.1,	N/A	A-F5-BIG--141019/73

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the Configuration utility login page may not follow best security practices when handling a malicious request. **CVE ID : CVE-2019-6651**		
Improper Input Validation	25-09-2019	3.3	On versions 14.0.0-14.1.2, 13.0.0-13.1.3, 12.1.0-12.1.5, and 11.5.1-11.6.5, the BIG-IP system fails to perform Martian Address Filtering (As defined in RFC 1812 section 5.3.7) on the control plane (management interface). This may allow attackers on an adjacent system to force BIG-IP into processing packets with spoofed source addresses. **CVE ID : CVE-2019-6654**	N/A	A-F5-BIG--141019/74
Information Exposure	25-09-2019	4.3	On versions 13.0.0-13.1.0.1, 12.1.0-12.1.4.1, 11.6.1-11.6.4, and 11.5.1-11.5.9, BIG-IP platforms where AVR, ASM, APM, PEM, AFM, and/or AAM is provisioned may leak sensitive data. **CVE ID : CVE-2019-6655**	N/A	A-F5-BIG--141019/75
big-ip_domain_name_system					
Information Exposure Through Discrepancy	25-09-2019	5	In BIG-IP 15.0.0, 14.1.0-14.1.0.6, 14.0.0-14.0.0.5, 13.0.0-13.1.1.5, 12.1.0-12.1.4.1, 11.5.1-11.6.4, BIG-IQ 7.0.0, 6.0.0-6.1.0,5.2.0-5.4.0, iWorkflow 2.3.0, and Enterprise Manager 3.1.1, the Configuration utility login page may not follow best security practices when	N/A	A-F5-BIG--141019/76

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			handling a malicious request. **CVE ID : CVE-2019-6651**		
Improper Input Validation	25-09-2019	3.3	On versions 14.0.0-14.1.2, 13.0.0-13.1.3, 12.1.0-12.1.5, and 11.5.1-11.6.5, the BIG-IP system fails to perform Martian Address Filtering (As defined in RFC 1812 section 5.3.7) on the control plane (management interface). This may allow attackers on an adjacent system to force BIG-IP into processing packets with spoofed source addresses. **CVE ID : CVE-2019-6654**	N/A	A-F5-BIG--141019/77
big-ip_edge_gateway					
Information Exposure Through Discrepancy	25-09-2019	5	In BIG-IP 15.0.0, 14.1.0-14.1.0.6, 14.0.0-14.0.0.5, 13.0.0-13.1.1.5, 12.1.0-12.1.4.1, 11.5.1-11.6.4, BIG-IQ 7.0.0, 6.0.0-6.1.0,5.2.0-5.4.0, iWorkflow 2.3.0, and Enterprise Manager 3.1.1, the Configuration utility login page may not follow best security practices when handling a malicious request. **CVE ID : CVE-2019-6651**	N/A	A-F5-BIG--141019/78
Improper Input Validation	25-09-2019	3.3	On versions 14.0.0-14.1.2, 13.0.0-13.1.3, 12.1.0-12.1.5, and 11.5.1-11.6.5, the BIG-IP system fails to perform Martian Address Filtering (As defined in RFC 1812 section 5.3.7) on the control plane (management	N/A	A-F5-BIG--141019/79

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interface). This may allow attackers on an adjacent system to force BIG-IP into processing packets with spoofed source addresses. **CVE ID : CVE-2019-6654**		
big-ip_fraud_protection_service					
Information Exposure Through Discrepancy	25-09-2019	5	In BIG-IP 15.0.0, 14.1.0-14.1.0.6, 14.0.0-14.0.0.5, 13.0.0-13.1.1.5, 12.1.0-12.1.4.1, 11.5.1-11.6.4, BIG-IQ 7.0.0, 6.0.0-6.1.0,5.2.0-5.4.0, iWorkflow 2.3.0, and Enterprise Manager 3.1.1, the Configuration utility login page may not follow best security practices when handling a malicious request. **CVE ID : CVE-2019-6651**	N/A	A-F5-BIG--141019/80
Improper Input Validation	25-09-2019	3.3	On versions 14.0.0-14.1.2, 13.0.0-13.1.3, 12.1.0-12.1.5, and 11.5.1-11.6.5, the BIG-IP system fails to perform Martian Address Filtering (As defined in RFC 1812 section 5.3.7) on the control plane (management interface). This may allow attackers on an adjacent system to force BIG-IP into processing packets with spoofed source addresses. **CVE ID : CVE-2019-6654**	N/A	A-F5-BIG--141019/81
big-ip_global_traffic_manager					
Information Exposure Through	25-09-2019	5	In BIG-IP 15.0.0, 14.1.0-14.1.0.6, 14.0.0-14.0.0.5, 13.0.0-13.1.1.5, 12.1.0-12.1.4.1, 11.5.1-11.6.4, BIG-	N/A	A-F5-BIG--141019/82

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Discrepancy			IQ 7.0.0, 6.0.0-6.1.0,5.2.0-5.4.0, iWorkflow 2.3.0, and Enterprise Manager 3.1.1, the Configuration utility login page may not follow best security practices when handling a malicious request. **CVE ID : CVE-2019-6651**		
Improper Input Validation	25-09-2019	3.3	On versions 14.0.0-14.1.2, 13.0.0-13.1.3, 12.1.0-12.1.5, and 11.5.1-11.6.5, the BIG-IP system fails to perform Martian Address Filtering (As defined in RFC 1812 section 5.3.7) on the control plane (management interface). This may allow attackers on an adjacent system to force BIG-IP into processing packets with spoofed source addresses. **CVE ID : CVE-2019-6654**	N/A	A-F5-BIG--141019/83
big-ip_link_controller					
Information Exposure Through Discrepancy	25-09-2019	5	In BIG-IP 15.0.0, 14.1.0-14.1.0.6, 14.0.0-14.0.0.5, 13.0.0-13.1.1.5, 12.1.0-12.1.4.1, 11.5.1-11.6.4, BIG-IQ 7.0.0, 6.0.0-6.1.0,5.2.0-5.4.0, iWorkflow 2.3.0, and Enterprise Manager 3.1.1, the Configuration utility login page may not follow best security practices when handling a malicious request. **CVE ID : CVE-2019-6651**	N/A	A-F5-BIG--141019/84
Improper Input	25-09-2019	3.3	On versions 14.0.0-14.1.2, 13.0.0-13.1.3, 12.1.0-12.1.5,	N/A	A-F5-BIG--141019/85

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			and 11.5.1-11.6.5, the BIG-IP system fails to perform Martian Address Filtering (As defined in RFC 1812 section 5.3.7) on the control plane (management interface). This may allow attackers on an adjacent system to force BIG-IP into processing packets with spoofed source addresses. **CVE ID : CVE-2019-6654**		
big-ip_local_traffic_manager					
Information Exposure Through Discrepancy	25-09-2019	5	In BIG-IP 15.0.0, 14.1.0-14.1.0.6, 14.0.0-14.0.0.5, 13.0.0-13.1.1.5, 12.1.0-12.1.4.1, 11.5.1-11.6.4, BIG-IQ 7.0.0, 6.0.0-6.1.0,5.2.0-5.4.0, iWorkflow 2.3.0, and Enterprise Manager 3.1.1, the Configuration utility login page may not follow best security practices when handling a malicious request. **CVE ID : CVE-2019-6651**	N/A	A-F5-BIG--141019/86
Improper Input Validation	25-09-2019	3.3	On versions 14.0.0-14.1.2, 13.0.0-13.1.3, 12.1.0-12.1.5, and 11.5.1-11.6.5, the BIG-IP system fails to perform Martian Address Filtering (As defined in RFC 1812 section 5.3.7) on the control plane (management interface). This may allow attackers on an adjacent system to force BIG-IP into processing packets with spoofed source addresses.	N/A	A-F5-BIG--141019/87

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-6654		
big-ip_policy_enforcement_manager					
Information Exposure Through Discrepancy	25-09-2019	5	In BIG-IP 15.0.0, 14.1.0-14.1.0.6, 14.0.0-14.0.0.5, 13.0.0-13.1.1.5, 12.1.0-12.1.4.1, 11.5.1-11.6.4, BIG-IQ 7.0.0, 6.0.0-6.1.0,5.2.0-5.4.0, iWorkflow 2.3.0, and Enterprise Manager 3.1.1, the Configuration utility login page may not follow best security practices when handling a malicious request. **CVE ID : CVE-2019-6651**	N/A	A-F5-BIG--141019/88
Improper Input Validation	25-09-2019	3.3	On versions 14.0.0-14.1.2, 13.0.0-13.1.3, 12.1.0-12.1.5, and 11.5.1-11.6.5, the BIG-IP system fails to perform Martian Address Filtering (As defined in RFC 1812 section 5.3.7) on the control plane (management interface). This may allow attackers on an adjacent system to force BIG-IP into processing packets with spoofed source addresses. **CVE ID : CVE-2019-6654**	N/A	A-F5-BIG--141019/89
Information Exposure	25-09-2019	4.3	On versions 13.0.0-13.1.0.1, 12.1.0-12.1.4.1, 11.6.1-11.6.4, and 11.5.1-11.5.9, BIG-IP platforms where AVR, ASM, APM, PEM, AFM, and/or AAM is provisioned may leak sensitive data. **CVE ID : CVE-2019-6655**	N/A	A-F5-BIG--141019/90
big-ip_webaccelerator					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure Through Discrepancy	25-09-2019	5	In BIG-IP 15.0.0, 14.1.0-14.1.0.6, 14.0.0-14.0.0.5, 13.0.0-13.1.1.5, 12.1.0-12.1.4.1, 11.5.1-11.6.4, BIG-IQ 7.0.0, 6.0.0-6.1.0,5.2.0-5.4.0, iWorkflow 2.3.0, and Enterprise Manager 3.1.1, the Configuration utility login page may not follow best security practices when handling a malicious request. **CVE ID : CVE-2019-6651**	N/A	A-F5-BIG--141019/91
Improper Input Validation	25-09-2019	3.3	On versions 14.0.0-14.1.2, 13.0.0-13.1.3, 12.1.0-12.1.5, and 11.5.1-11.6.5, the BIG-IP system fails to perform Martian Address Filtering (As defined in RFC 1812 section 5.3.7) on the control plane (management interface). This may allow attackers on an adjacent system to force BIG-IP into processing packets with spoofed source addresses. **CVE ID : CVE-2019-6654**	N/A	A-F5-BIG--141019/92
enterprise_manager					
Information Exposure Through Discrepancy	25-09-2019	5	In BIG-IP 15.0.0, 14.1.0-14.1.0.6, 14.0.0-14.0.0.5, 13.0.0-13.1.1.5, 12.1.0-12.1.4.1, 11.5.1-11.6.4, BIG-IQ 7.0.0, 6.0.0-6.1.0,5.2.0-5.4.0, iWorkflow 2.3.0, and Enterprise Manager 3.1.1, the Configuration utility login page may not follow best security practices when handling a malicious	N/A	A-F5-ENTE-141019/93

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			request. **CVE ID : CVE-2019-6651**		
big-iq_centralized_management					
Information Exposure Through Discrepancy	25-09-2019	5	In BIG-IP 15.0.0, 14.1.0-14.1.0.6, 14.0.0-14.0.0.5, 13.0.0-13.1.1.5, 12.1.0-12.1.4.1, 11.5.1-11.6.4, BIG-IQ 7.0.0, 6.0.0-6.1.0,5.2.0-5.4.0, iWorkflow 2.3.0, and Enterprise Manager 3.1.1, the Configuration utility login page may not follow best security practices when handling a malicious request. **CVE ID : CVE-2019-6651**	N/A	A-F5-BIG--141019/94
Improper Authentication	25-09-2019	6.4	In BIG-IQ 6.0.0-6.1.0, services for stats do not require authentication nor do they implement any form of Transport Layer Security (TLS). **CVE ID : CVE-2019-6652**	N/A	A-F5-BIG--141019/95
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-09-2019	3.5	There is a Stored Cross Site Scripting vulnerability in the undisclosed page of a BIG-IQ 6.0.0-6.1.0 or 5.2.0-5.4.0 system. The attack can be stored by users granted the Device Manager and Administrator roles. **CVE ID : CVE-2019-6653**	N/A	A-F5-BIG--141019/96
iworkflow					
Information Exposure Through Discrepancy	25-09-2019	5	In BIG-IP 15.0.0, 14.1.0-14.1.0.6, 14.0.0-14.0.0.5, 13.0.0-13.1.1.5, 12.1.0-12.1.4.1, 11.5.1-11.6.4, BIG-IQ 7.0.0, 6.0.0-6.1.0,5.2.0-	N/A	A-F5-IWOR-141019/97

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			5.4.0, iWorkflow 2.3.0, and Enterprise Manager 3.1.1, the Configuration utility login page may not follow best security practices when handling a malicious request. **CVE ID : CVE-2019-6651**		
firegiant					
wix_toolset					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	19-09-2019	5.8	An issue was discovered in DTF in FireGiant WiX Toolset before 3.11.2. Microsoft.Deployment.Compression.Cab.dll and Microsoft.Deployment.Compression.Zip.dll allow directory traversal during CAB or ZIP archive extraction, because the full name of an archive file (even with a ../ sequence) is concatenated with the destination path. **CVE ID : CVE-2019-16511**	N/A	A-FIR-WIX_-141019/98
forcepoint					
vpn_client					
Unquoted Search Path or Element	20-09-2019	7.2	Forcepoint VPN Client for Windows versions lower than 6.6.1 have an unquoted search path vulnerability. This enables local privilege escalation to SYSTEM user. By default, only local administrators can write executables to the vulnerable directories. Forcepoint thanks Peleg Hadar of SafeBreach Labs for	https://support.forcepoint.com/KBArticle?id=000017525	A-FOR-VPN_-141019/99

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			finding this vulnerability and for reporting it to us. **CVE ID : CVE-2019-6145**		
Freeipa					
freeipa					
Insufficient Session Expiration	17-09-2019	2.1	A flaw was found in FreeIPA versions 4.5.0 and later. Session cookies were retained in the cache after logout. An attacker could abuse this flaw if they obtain previously valid session cookies and can use this to gain access to the session. **CVE ID : CVE-2019-14826**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-14826	A-FRE-FREE-141019/100
geautomation					
proficy					
Improper Input Validation	16-09-2019	5	Emerson GE Automation Proficy Machine Edition 8.0 allows an access violation and application crash via crafted traffic from a remote device, as demonstrated by an RX7i device. **CVE ID : CVE-2019-16353**	N/A	A-GEA-PROF-141019/101
gilacms					
gila_cms					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-09-2019	4	Gila CMS before 1.11.1 allows admin/fm/?f=../ directory traversal, leading to Local File Inclusion. **CVE ID : CVE-2019-16679**	N/A	A-GIL-GILA-141019/102
Gitlab					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
gitlab					
Incorrect Permission Assignment for Critical Resource	16-09-2019	5.5	An issue was discovered in GitLab Community and Enterprise Edition 10.8 through 12.2.1. An internal endpoint unintentionally allowed group maintainers to view and edit group runner settings. **CVE ID : CVE-2019-15721**	https://about.gitlab.com/2019/08/29/security-release-gitlab-12-dot-2-dot-3-released/	A-GIT-GITL-141019/103
Uncontrolled Resource Consumption	16-09-2019	5	An issue was discovered in GitLab Community and Enterprise Edition 8.15 through 12.2.1. Particular mathematical expressions in GitLab Markdown can exhaust client resources. **CVE ID : CVE-2019-15722**	https://about.gitlab.com/2019/08/29/security-release-gitlab-12-dot-2-dot-3-released/	A-GIT-GITL-141019/104
Incorrect Permission Assignment for Critical Resource	16-09-2019	5	An issue was discovered in GitLab Community and Enterprise Edition 11.9.x and 11.10.x before 11.10.1. Merge requests created by email could be used to bypass push rules in certain situations. **CVE ID : CVE-2019-15723**	https://about.gitlab.com/2019/08/29/security-release-gitlab-12-dot-2-dot-3-released/	A-GIT-GITL-141019/105
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	16-09-2019	4.3	An issue was discovered in GitLab Community and Enterprise Edition 11.10 through 12.2.1. Label descriptions are vulnerable to HTML injection. **CVE ID : CVE-2019-15724**	https://about.gitlab.com/2019/08/29/security-release-gitlab-12-dot-2-dot-3-released/	A-GIT-GITL-141019/106
Information Exposure	16-09-2019	5	An issue was discovered in GitLab Community and Enterprise Edition 12.0	N/A	A-GIT-GITL-141019/107

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			through 12.2.1. An IDOR in the epic notes API that could result in disclosure of private milestones, labels, and other information. **CVE ID : CVE-2019-15725**		
Information Exposure	16-09-2019	5	An issue was discovered in GitLab Community and Enterprise Edition through 12.2.1. Embedded images and media files in markdown could be pointed to an arbitrary server, which would reveal the IP address of clients requesting the file from that server. **CVE ID : CVE-2019-15726**	https://about.gitlab.com/2019/08/29/security-release-gitlab-12-dot-2-dot-3-released/	A-GIT-GITL-141019/108
Information Exposure	16-09-2019	5	An issue was discovered in GitLab Community and Enterprise Edition 11.2 through 12.2.1. Insufficient permission checks were being applied when displaying CI results, potentially exposing some CI metrics data to unauthorized users. **CVE ID : CVE-2019-15727**	https://about.gitlab.com/2019/08/29/security-release-gitlab-12-dot-2-dot-3-released/	A-GIT-GITL-141019/109
Server-Side Request Forgery (SSRF)	16-09-2019	5	An issue was discovered in GitLab Community and Enterprise Edition 10.1 through 12.2.1. Protections against SSRF attacks on the Kubernetes integration are insufficient, which could have allowed an attacker to request any local network resource accessible from the GitLab server.	N/A	A-GIT-GITL-141019/110

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-15728		
Information Exposure	17-09-2019	5	An issue was discovered in GitLab Community and Enterprise Edition 8.18 through 12.2.1. An internal endpoint unintentionally disclosed information about the last pipeline that ran for a merge request. **CVE ID : CVE-2019-15729**	N/A	A-GIT-GITL-141019/111
Server-Side Request Forgery (SSRF)	16-09-2019	5	An issue was discovered in GitLab Community and Enterprise Edition 8.14 through 12.2.1. The Jira integration contains a SSRF vulnerability as a result of a bypass of the current protection mechanisms against this type of attack, which would allow sending requests to any resources accessible in the local network by the GitLab server. **CVE ID : CVE-2019-15730**	N/A	A-GIT-GITL-141019/112
Incorrect Permission Assignment for Critical Resource	16-09-2019	5	An issue was discovered in GitLab Community and Enterprise Edition 12.0 through 12.2.1. Non-members were able to comment on merge requests despite the repository being set to allow only project members to do so. **CVE ID : CVE-2019-15731**	https://about.gitlab.com/2019/08/29/security-release-gitlab-12-dot-2-dot-3-released/	A-GIT-GITL-141019/113
Information Exposure	16-09-2019	5	An issue was discovered in GitLab Community and Enterprise Edition 12.2 through 12.2.1. The project	https://about.gitlab.com/2019/08/29/securit	A-GIT-GITL-141019/114

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			import API could be used to bypass project visibility restrictions. **CVE ID : CVE-2019-15732**	y-release-gitlab-12-dot-2-dot-3-released/	
Information Exposure	16-09-2019	4	An issue was discovered in GitLab Community and Enterprise Edition 7.12 through 12.2.1. The specified default branch name could be exposed to unauthorized users. **CVE ID : CVE-2019-15733**	https://about.gitlab.com/2019/08/29/security-release-gitlab-12-dot-2-dot-3-released/	A-GIT-GITL-141019/115
Information Exposure	16-09-2019	4	An issue was discovered in GitLab Community and Enterprise Edition 8.6 through 12.2.1. Under very specific conditions, commit titles and team member comments could become viewable to users who did not have permission to access these. **CVE ID : CVE-2019-15734**	https://about.gitlab.com/2019/08/29/security-release-gitlab-12-dot-2-dot-3-released/	A-GIT-GITL-141019/116
Uncontrolled Resource Consumption	16-09-2019	5	An issue was discovered in GitLab Community and Enterprise Edition through 12.2.1. Under certain circumstances, CI pipelines could potentially be used in a denial of service attack. **CVE ID : CVE-2019-15736**	https://about.gitlab.com/2019/08/29/security-release-gitlab-12-dot-2-dot-3-released/	A-GIT-GITL-141019/117
Improper Authentication	16-09-2019	6.4	An issue was discovered in GitLab Community and Enterprise Edition through 12.2.1. Certain account actions needed improved authentication and session management.	https://about.gitlab.com/2019/08/29/security-release-gitlab-12-dot-2-dot-	A-GIT-GITL-141019/118

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-15737	3-released/	
Information Exposure	16-09-2019	5	An issue was discovered in GitLab Community and Enterprise Edition 12.0 through 12.2.1. Under certain conditions, merge request IDs were being disclosed via email. **CVE ID : CVE-2019-15738**	https://about.gitlab.com/2019/08/29/security-release-gitlab-12-dot-2-dot-3-released/	A-GIT-GITL-141019/119
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-09-2019	4.3	An issue was discovered in GitLab Community and Enterprise Edition 8.1 through 12.2.1. Certain areas displaying Markdown were not properly sanitizing some XSS payloads. **CVE ID : CVE-2019-15739**	https://about.gitlab.com/2019/08/29/security-release-gitlab-12-dot-2-dot-3-released/	A-GIT-GITL-141019/120
Information Exposure	16-09-2019	5	An issue was discovered in GitLab Community and Enterprise Edition 7.9 through 12.2.1. EXIF Geolocation data was not being removed from certain image uploads. **CVE ID : CVE-2019-15740**	N/A	A-GIT-GITL-141019/121
Incorrect Permission Assignment for Critical Resource	16-09-2019	5.5	An issue was discovered in GitLab Enterprise Edition 11.x and 12.x before 12.0.9, 12.1.x before 12.1.9, and 12.2.x before 12.2.5. It has Incorrect Access Control. **CVE ID : CVE-2019-16170**	N/A	A-GIT-GITL-141019/122
gnucobol_project					
gnucobol					
Buffer Copy without Checking Size of Input	17-09-2019	6.8	GnuCOBOL 2.2 has a stack-based buffer overflow in the cb_name() function in cobc/tree.c via crafted	N/A	A-GNU-GNUC-141019/123

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			COBOL source code. **CVE ID : CVE-2019-16395**		
Use After Free	17-09-2019	6.8	GnuCOBOL 2.2 has a use-after-free in the end_scope_of_program_name() function in cobc/parser.y via crafted COBOL source code. **CVE ID : CVE-2019-16396**	N/A	A-GNU-GNUC-141019/124
Gradle					
gradle					
Improper Input Validation	16-09-2019	4.3	The PGP signing plugin in Gradle before 6.0 relies on the SHA-1 algorithm, which might allow an attacker to replace an artifact with a different one that has the same SHA-1 message digest, a related issue to CVE-2005-4900. **CVE ID : CVE-2019-16370**	N/A	A-GRA-GRAD-141019/125
grafana					
grafana					
Insufficiently Protected Credentials	23-09-2019	4	An issue was discovered in Grafana 5.4.0. Passwords for data sources used by Grafana (e.g., MySQL) are not encrypted. An admin user can reveal passwords for any data source by pressing the "Save and test" button within a data source's settings menu. When watching the transaction with Burp Proxy, the password for the data source is revealed and sent to the	N/A	A-GRA-GRAF-141019/126

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			server. From a browser, a prompt to save the credentials is generated, and the password can be revealed by simply checking the "Show password" box. **CVE ID : CVE-2019-15635**		
halo					
halo					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-09-2019	3.5	Halo 1.1.0 has XSS via a crafted authorUrl in JSON data to api/content/posts/comments. **CVE ID : CVE-2019-16890**	N/A	A-HAL-HALO-141019/127
Haxx					
curl					
Double Free	16-09-2019	7.5	Double-free vulnerability in the FTP-kerberos code in cURL 7.52.0 to 7.65.3. **CVE ID : CVE-2019-5481**	N/A	A-HAX-CURL-141019/128
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-09-2019	7.5	Heap buffer overflow in the TFTP protocol handler in cURL 7.19.4 to 7.65.3. **CVE ID : CVE-2019-5482**	N/A	A-HAX-CURL-141019/129
hcltech					
appscan_source					
Improper Restriction of XML External Entity	25-09-2019	5.8	HCL AppScan Source before 9.03.13 is susceptible to XML External Entity (XXE) attacks in multiple locations. In particular, an attacker can	https://hclpnpsupport.hcltech.com/csm?id=kb_article&sys	A-HCL-APPS-141019/130

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reference ('XXE')			send a specially crafted .ozasmt file to a targeted victim and ask the victim to open it. When the victim imports the .ozasmt file in AppScan Source, the content of any file in the local file system (to which the victim as read access) can be exfiltrated to a remote listener under the attacker's control. The product does not disable external XML Entity Processing, which can lead to information disclosure and denial of services attacks. **CVE ID : CVE-2019-16188**	_id=0812a9961b0c885077761fc58d4bcb06	
hongcms_project					
hongcms					
Improper Input Validation	25-09-2019	5.5	HongCMS 3.0.0 allows arbitrary file deletion via a ../ in the file parameter to admin/index.php/database/ajax?action=delete, a similar issue to CVE-2018-16774. (If the attacker deletes config.php and visits install/index.php, they can reinstall the product.) **CVE ID : CVE-2019-16867**	N/A	A-HON-HONG-141019/131
hrworks					
hrworks					
Improper Neutralization of Input During Web Page Generation	17-09-2019	4.3	A reflected Cross-site scripting (XSS) vulnerability in HRworks V 1.16.1 allows remote attackers to inject arbitrary web script or HTML via the URL	N/A	A-HRW-HRWO-141019/132

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			parameter to the Login component. **CVE ID : CVE-2019-11559**		
html-pdf_project					
html-pdf					
Information Exposure	20-09-2019	5	The html-pdf package 2.2.0 for Node.js has an arbitrary file read vulnerability via an HTML file that uses XMLHttpRequest to access a file:/// URL. **CVE ID : CVE-2019-15138**	N/A	A-HTM-HTML-141019/133
hunspell_project					
hunspell					
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-09-2019	4.3	Hunspell 1.7.0 has an invalid read operation in SuggestMgr::leftcommonsubstring in suggestmgr.cxx. **CVE ID : CVE-2019-16707**	N/A	A-HUN-HUNS-141019/134
IBM					
cognos_analytics					
Uncontrolled Resource Consumption	17-09-2019	7.8	IBM Cognos Analytics 11.0, and 11.1 is vulnerable to a denial of service attack that could allow a remote user to send specially crafted requests that would consume all available CPU and memory resources. IBM X-Force ID: 158973. **CVE ID : CVE-2019-4183**	https://www.ibm.com/support/pages/node/1073530	A-IBM-COGN-141019/135
Improper Neutralization of Input	17-09-2019	3.5	IBM Cognos Analytics 11.0 and 11.1 is vulnerable to cross-site scripting. This	https://www.ibm.com/support/pa	A-IBM-COGN-141019/136

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			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: 161421. **CVE ID : CVE-2019-4342**	ges/node/1073530	
mq					
Improper Input Validation	26-09-2019	4	IBM MQ 7.5.0.0 - 7.5.0.9, 7.1.0.0 - 7.1.0.9, 8.0.0.0 - 8.0.0.12, 9.0.0.0 - 9.0.0.6, 9.1.0.0 - 9.1.0.2, and 9.1.0 - 9.1.2 command server is vulnerable to a denial of service attack caused by an authenticated and authorized user using specially crafted PCF messages. IBM X-Force ID: 162084. **CVE ID : CVE-2019-4378**	https://supportcontent.ibm.com/support/pages/node/886885	A-IBM-MQ-141019/137
application_performance_management					
Improper Restriction of Rendered UI Layers or Frames	17-09-2019	4.3	IBM Cloud Application Performance Management 8.1.4 could allow a remote attacker to hijack the clicking action of the victim. By persuading a victim to visit a malicious Web site, a remote attacker could exploit this vulnerability to hijack the victim's click actions and possibly launch further attacks against the victim. IBM X-Force ID: 157509.	https://www.ibm.com/support/pages/security-bulletin-ibm-application-performance-management-could-allow-remote-attacker-	A-IBM-APPL-141019/138

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-4086	hijack-clicking-action-victim-cve-2019-4086	
cognos_controller					
Inadequate Encryption Strength	17-09-2019	5	IBM Cognos Controller 10.3.0, 10.3.1, 10.4.0, and 10.4.1 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 158880. **CVE ID : CVE-2019-4175**	https://www.ibm.com/support/pages/security-bulletin-security-vulnerabilities-exist-ibm-cognos-controller	A-IBM-COGN-141019/139
Information Exposure	17-09-2019	4.3	IBM Cognos Controller 10.3.0, 10.3.1, 10.4.0, and 10.4.1 does not set the secure attribute on authorization tokens or session cookies. This could allow an attacker to obtain sensitive information using man in the middle techniques. IBM X-Force ID: 158876. **CVE ID : CVE-2019-4171**	https://www.ibm.com/support/pages/security-bulletin-security-vulnerabilities-exist-ibm-cognos-controller	A-IBM-COGN-141019/140
sterling_file_gateway					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-09-2019	6.5	IBM Sterling File Gateway 2.2.0.0 through 6.0.1.0 is vulnerable to SQL injection. A remote attacker could send specially-crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end	https://www.ibm.com/support/pages/security-bulletin-sql-injection-vulnerability-affects-	A-IBM-STER-141019/141

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			database. IBM X-Force ID: 158413. **CVE ID : CVE-2019-4147**	ibm-sterling-file-gateway-cve-2019-4147	
security_key_lifecycle_manager					
Cross-Site Request Forgery (CSRF)	24-09-2019	4.3	IBM Security Key Lifecycle Manager 3.0 and 3.0.1 is 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: 165137. **CVE ID : CVE-2019-4515**	https://www.ibm.com/support/pages/node/290671	A-IBM-SECU-141019/142
Weak Password Requirements	20-09-2019	5	IBM Security Key Lifecycle Manager 3.0 and 3.0.1 does not require that users should have strong passwords by default, which makes it easier for attackers to compromise user accounts. IBM X-Force ID: 166626. **CVE ID : CVE-2019-4565**	https://www.ibm.com/support/pages/security-bulletin-ibm-security-key-lifecycle-manager-uses-weak-password-policy-cve-2019-4565	A-IBM-SECU-141019/143
Cleartext Storage of Sensitive Information	24-09-2019	2.1	IBM Security Key Lifecycle Manager 3.0 and 3.0.1 stores user credentials in plain in clear text which can be read by a local user. IBM X-Force ID: 166627. **CVE ID : CVE-2019-4566**	https://www.ibm.com/support/pages/node/1074344	A-IBM-SECU-141019/144
websphere_application_server					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	17-09-2019	4	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 could allow a user with access to audit logs to obtain sensitive information, caused by improper handling of command line options. IBM X-Force ID: 163997. **CVE ID : CVE-2019-4477**	https://www.ibm.com/support/pages/node/960290	A-IBM-WEBS-141019/145
Information Exposure	20-09-2019	5	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 Network Deployment could allow a remote attacker to obtain sensitive information, caused by sending a specially-crafted URL. This can lead the attacker to view any file in a certain directory. IBM X-Force ID: 164364. **CVE ID : CVE-2019-4505**	https://www.ibm.com/support/pages/node/964766	A-IBM-WEBS-141019/146
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-09-2019	5	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 could allow a remote attacker to traverse directories on the system. An attacker could send a specially-crafted URL containing "dot dot" sequences (/../) to view arbitrary files on the system. IBM X-Force ID: 160201. **CVE ID : CVE-2019-4268**	https://www.ibm.com/support/pages/node/884030	A-IBM-WEBS-141019/147
Improper Neutralization of Input During Web Page	17-09-2019	3.5	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 Admin Console is vulnerable to cross-site scripting. This vulnerability allows users to	https://www.ibm.com/support/pages/node/884036	A-IBM-WEBS-141019/148

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			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: 160203. **CVE ID : CVE-2019-4270**		
Improper Input Validation	17-09-2019	3.5	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 Admin console is vulnerable to a Client-side HTTP parameter pollution vulnerability. IBM X-Force ID: 160243. **CVE ID : CVE-2019-4271**	https://www.ibm.com/support/pages/node/884040	A-IBM-WEBS-141019/149
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-09-2019	4	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9,0 could allow a remote attacker to traverse directories on the file system. An attacker could send a specially-crafted URL request to view arbitrary files on the system but not content. IBM X-Force ID: 163226. **CVE ID : CVE-2019-4442**	https://www.ibm.com/support/pages/node/959021	A-IBM-WEBS-141019/150
websphere_virtual_enterprise					
Information Exposure	20-09-2019	5	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 Network Deployment could allow a remote attacker to obtain sensitive information, caused by sending a specially-crafted URL. This can lead the attacker to view any file in a certain	https://www.ibm.com/support/pages/node/964766	A-IBM-WEBS-141019/151

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			directory. IBM X-Force ID: 164364. **CVE ID : CVE-2019-4505**		
content_navigator					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-09-2019	3.5	IBM Content Navigator 3.0CD is 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: 166721. **CVE ID : CVE-2019-4571**	https://www.ibm.com/support/pages/node/1073576	A-IBM-CONT-141019/152
qradar_security_information_and_event_manager					
Server-Side Request Forgery (SSRF)	26-09-2019	5	IBM QRadar SIEM 7.2 and 7.3 is vulnerable to Server Side Request Forgery (SSRF). This may allow an unauthenticated attacker to send unauthorized requests from the QRadar system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 160014. **CVE ID : CVE-2019-4262**	https://www.ibm.com/support/pages/node/1074538	A-IBM-QRAD-141019/153
idreamsoft					
icms					
Cross-Site Request Forgery (CSRF)	21-09-2019	5.8	An issue was discovered in idreamsoft iCMS V7.0. admincp.php?app=members&do=del allows CSRF. **CVE ID : CVE-2019-16677**	N/A	A-IDR-ICMS-141019/154

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Imagemagick					
imagemagick					
Missing Release of Resource after Effective Lifetime	23-09-2019	4.3	ImageMagick 7.0.8-35 has a memory leak in coders/dot.c, as demonstrated by AcquireMagickMemory in MagickCore/memory.c. **CVE ID : CVE-2019-16710**	N/A	A-IMA-IMAG-141019/155
Missing Release of Resource after Effective Lifetime	23-09-2019	4.3	ImageMagick 7.0.8-40 has a memory leak in Huffman2DEncodeImage in coders/ps2.c. **CVE ID : CVE-2019-16711**	N/A	A-IMA-IMAG-141019/156
Missing Release of Resource after Effective Lifetime	23-09-2019	4.3	ImageMagick 7.0.8-43 has a memory leak in Huffman2DEncodeImage in coders/ps3.c, as demonstrated by WritePS3Image. **CVE ID : CVE-2019-16712**	N/A	A-IMA-IMAG-141019/157
Missing Release of Resource after Effective Lifetime	23-09-2019	4.3	ImageMagick 7.0.8-43 has a memory leak in coders/dot.c, as demonstrated by PingImage in MagickCore/constitute.c. **CVE ID : CVE-2019-16713**	N/A	A-IMA-IMAG-141019/158
Missing Release of Resource after Effective Lifetime	23-09-2019	4.3	ImageMagick 7.0.8-35 has a memory leak in magick/xwindow.c, related to XCreateImage. **CVE ID : CVE-2019-16708**	N/A	A-IMA-IMAG-141019/159
Missing Release of Resource after	23-09-2019	4.3	ImageMagick 7.0.8-35 has a memory leak in coders/dps.c, as demonstrated by	N/A	A-IMA-IMAG-141019/160

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Effective Lifetime			XCreateImage. **CVE ID : CVE-2019-16709**		
Infradead					
openconnect					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-09-2019	7.5	process_http_response in OpenConnect before 8.05 has a Buffer Overflow when a malicious server uses HTTP chunked encoding with crafted chunk sizes. **CVE ID : CVE-2019-16239**	N/A	A-INF-OPEN-141019/161
inoideas					
inoerp					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-09-2019	7.5	download.php in inoERP 4.15 allows SQL injection through insecure deserialization. **CVE ID : CVE-2019-16894**	N/A	A-INO-INOE-141019/162
integard_pro_project					
integard_pro					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-09-2019	7.5	Integard Pro 2.2.0.9026 allows remote attackers to execute arbitrary code via a buffer overflow involving a long NoJs parameter to the /LoginAdmin URI. **CVE ID : CVE-2019-16702**	N/A	A-INT-INTE-141019/163
Intel					
easy_streaming_wizard					
Improper Privilege Management	16-09-2019	4.6	Improper file permissions in the installer for Intel(R) Easy Streaming Wizard before	https://www.intel.com/content/w	A-INT-EASY-141019/164

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			version 2.1.0731 may allow an authenticated user to potentially enable escalation of privilege via local attack. **CVE ID : CVE-2019-11166**	ww/us/en/security-center/advisory/intel-sa-00285.html	
Ipswitch					
moveit_transfer					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	24-09-2019	6.4	MOVEit.DMZ.WebApi.dll in Progress MOVEit Transfer 2018 SP2 before 10.2.4, 2019 before 11.0.2, and 2019.1 before 11.1.1 allows an unauthenticated attacker to gain unauthorized access to the database. Depending on the database engine being used (MySQL, Microsoft SQL Server, or Azure SQL), an attacker may be able to infer information about the structure and contents of the database, or may be able to alter the database via the REST API, aka SQL Injection. **CVE ID : CVE-2019-16383**	https://docs.ipswitch.com/MOVEit/Transfer2019_1/ReleaseNotes/en/index.htm#49443.htm	A-IPS-MOVE-141019/165
Irfanview					
irfanview					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	25-09-2019	6.8	In IrfanView 4.53, Data from a Faulting Address controls a subsequent Write Address starting at image00400000+0x000000000001dcfc. **CVE ID : CVE-2019-16887**	N/A	A-IRF-IRFA-141019/166
Jenkins					
aqua_security_scanner					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Cleartext Transmission of Sensitive Information	25-09-2019	5	Jenkins Aqua Security Scanner Plugin 3.0.17 and earlier transmitted configured credentials in plain text as part of the global Jenkins configuration form, potentially resulting in their exposure. **CVE ID : CVE-2019-10428**	https://jenkins.io/security/advisory/2019-09-25/#SECURITY-1508	A-JEN-AQUA-141019/167
jenkins					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-09-2019	3.5	In Jenkins 2.196 and earlier, LTS 2.176.3 and earlier, the f:expandableTextBox form control interpreted its content as HTML when expanded, resulting in a stored XSS vulnerability exploitable by users with permission to define its contents (typically Job/Configure). **CVE ID : CVE-2019-10401**	https://jenkins.io/security/advisory/2019-09-25/#SECURITY-1498	A-JEN-JENK-141019/168
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-09-2019	3.5	In Jenkins 2.196 and earlier, LTS 2.176.3 and earlier, the f:combobox form control interpreted its item labels as HTML, resulting in a stored XSS vulnerability exploitable by users with permission to define its contents. **CVE ID : CVE-2019-10402**	https://jenkins.io/security/advisory/2019-09-25/#SECURITY-1525	A-JEN-JENK-141019/169
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-09-2019	3.5	Jenkins 2.196 and earlier, LTS 2.176.3 and earlier did not escape the SCM tag name on the tooltip for SCM tag actions, resulting in a stored XSS vulnerability exploitable by users able to control SCM tag names for these actions.	https://jenkins.io/security/advisory/2019-09-25/#SECURITY-1537%20(1)	A-JEN-JENK-141019/170

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10403		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-09-2019	3.5	Jenkins 2.196 and earlier, LTS 2.176.3 and earlier did not escape the reason why a queue items is blcoked in tooltips, resulting in a stored XSS vulnerability exploitable by users able to control parts of the reason a queue item is blocked, such as label expressions not matching any idle executors. **CVE ID : CVE-2019-10404**	https://jenkins.io/security/advisory/2019-09-25/#SECURITY-1537%20(2)	A-JEN-JENK-141019/171
Information Exposure	25-09-2019	4	Jenkins 2.196 and earlier, LTS 2.176.3 and earlier printed the value of the "Cookie" HTTP request header on the /whoAmI/ URL, allowing attackers exploiting another XSS vulnerability to obtain the HTTP session cookie despite it being marked HttpOnly. **CVE ID : CVE-2019-10405**	https://jenkins.io/security/advisory/2019-09-25/#SECURITY-1505	A-JEN-JENK-141019/172
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-09-2019	3.5	Jenkins 2.196 and earlier, LTS 2.176.3 and earlier did not restrict or filter values set as Jenkins URL in the global configuration, resulting in a stored XSS vulnerability exploitable by attackers with Overall/Administer permission. **CVE ID : CVE-2019-10406**	https://jenkins.io/security/advisory/2019-09-25/#SECURITY-1471	A-JEN-JENK-141019/173
inheritance-plugin					
Information Exposure	25-09-2019	4	Jenkins Project Inheritance Plugin 2.0.0 and earlier displayed a list of	https://jenkins.io/security/advisor	A-JEN-INHE-141019/174

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			environment variables passed to a build without masking sensitive variables contributed by the Mask Passwords Plugin. **CVE ID : CVE-2019-10407**	y/2019-09-25/#SECURITY-351	
project_inheritance					
Incorrect Authorization	25-09-2019	4	A cross-site request forgery vulnerability in Jenkins Project Inheritance Plugin 2.0.0 and earlier allowed attackers to trigger project generation from templates. **CVE ID : CVE-2019-10408**	https://jenkins.io/security/advisory/2019-09-25/#SECURITY-401	A-JEN-PROJ-141019/175
log_parser					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-09-2019	3.5	Jenkins Log Parser Plugin 2.0 and earlier did not escape an error message, resulting in a cross-site scripting vulnerability exploitable by users able to define log parsing rules. **CVE ID : CVE-2019-10410**	https://jenkins.io/security/advisory/2019-09-25/#SECURITY-732	A-JEN-LOG_-141019/176
inedo_buildmaster					
Cleartext Transmission of Sensitive Information	25-09-2019	5	Jenkins Inedo BuildMaster Plugin 2.4.0 and earlier transmitted configured credentials in plain text as part of the global Jenkins configuration form, potentially resulting in their exposure. **CVE ID : CVE-2019-10411**	https://jenkins.io/security/advisory/2019-09-25/#SECURITY-1513	A-JEN-INED-141019/177
inedo_proget					
Cleartext Transmission of Sensitive	25-09-2019	5	Jenkins Inedo ProGet Plugin 1.2 and earlier transmitted configured credentials in	https://jenkins.io/security/advisor	A-JEN-INED-141019/178

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information			plain text as part of the global Jenkins configuration form, potentially resulting in their exposure. **CVE ID : CVE-2019-10412**	y/2019-09-25/#SECURITY-1514	
data_theorem_mobile_app_security					
Cleartext Storage of Sensitive Information	25-09-2019	4	Jenkins Data Theorem: CI/CD Plugin 1.3 and earlier stored credentials unencrypted in job config.xml files on the Jenkins master where they could be viewed by users with Extended Read permission, or access to the master file system. **CVE ID : CVE-2019-10413**	https://jenkins.io/security/advisory/2019-09-25/#SECURITY-1557	A-JEN-DATA-141019/179
git_changelog					
Cleartext Storage of Sensitive Information	25-09-2019	3.5	Jenkins Git Changelog Plugin 2.17 and earlier stored credentials unencrypted in job config.xml files on the Jenkins master where they could be viewed by users with Extended Read permission, or access to the master file system. **CVE ID : CVE-2019-10414**	https://jenkins.io/security/advisory/2019-09-25/#SECURITY-1574	A-JEN-GIT_-141019/180
violation_comments_to_gitlab					
Cleartext Storage of Sensitive Information	25-09-2019	4	Jenkins Violation Comments to GitLab Plugin 2.28 and earlier stored credentials unencrypted in its global configuration file on the Jenkins master where they could be viewed by users with access to the master file system.	https://jenkins.io/security/advisory/2019-09-25/#SECURITY-1577	A-JEN-VIOL-141019/181

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10415		
Cleartext Storage of Sensitive Information	25-09-2019	4	Jenkins Violation Comments to GitLab Plugin 2.28 and earlier stored credentials unencrypted in job config.xml files on the Jenkins master where they could be viewed by users with Extended Read permission, or access to the master file system. **CVE ID : CVE-2019-10416**	https://jenkins.io/security/advisory/2019-09-25/#SECURITY-1577	A-JEN-VIOL-141019/182
kubernetes_pipeline					
Improper Privilege Management	25-09-2019	6.5	Jenkins Kubernetes :: Pipeline :: Kubernetes Steps Plugin provides a custom whitelist for script security that allowed attackers to invoke arbitrary methods, bypassing typical sandbox protection. **CVE ID : CVE-2019-10417**	https://jenkins.io/security/advisory/2019-09-25/#SECURITY-920%20(1)	A-JEN-KUBE-141019/183
Improper Privilege Management	25-09-2019	6.5	Jenkins Kubernetes :: Pipeline :: Arquillian Steps Plugin provides a custom whitelist for script security that allowed attackers to invoke arbitrary methods, bypassing typical sandbox protection. **CVE ID : CVE-2019-10418**	https://jenkins.io/security/advisory/2019-09-25/#SECURITY-920%20(2)	A-JEN-KUBE-141019/184
vfabric_application_director					
Cleartext Storage of Sensitive Information	25-09-2019	2.1	Jenkins vFabric Application Director Plugin stores credentials unencrypted in its global configuration file on the Jenkins master where they can be viewed by users	https://jenkins.io/security/advisory/2019-09-25/#SECURTIY-1541	A-JEN-VFAB-141019/185

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with access to the master file system. **CVE ID : CVE-2019-10419**		
assembla					
Cleartext Storage of Sensitive Information	25-09-2019	2.1	Jenkins Assembla Plugin stores credentials unencrypted in its global configuration file on the Jenkins master where they can be viewed by users with access to the master file system. **CVE ID : CVE-2019-10420**	https://jenkins.io/security/advisory/2019-09-25/#SECURITY-1543	A-JEN-ASSE-141019/186
azure_event_grid_notifier					
Cleartext Storage of Sensitive Information	25-09-2019	4	Jenkins Azure Event Grid Build Notifier Plugin stores credentials unencrypted in job config.xml files on the Jenkins master where they can be viewed by users with Extended Read permission, or access to the master file system. **CVE ID : CVE-2019-10421**	https://jenkins.io/security/advisory/2019-09-25/#SECURITY-1544	A-JEN-AZUR-141019/187
call_remote_job					
Cleartext Storage of Sensitive Information	25-09-2019	4	Jenkins Call Remote Job Plugin stores credentials unencrypted in job config.xml files on the Jenkins master where they can be viewed by users with Extended Read permission, or access to the master file system. **CVE ID : CVE-2019-10422**	https://jenkins.io/security/advisory/2019-09-25/#SECURITY-1548	A-JEN-CALL-141019/188
codescan					
Cleartext	25-09-2019	2.1	Jenkins CodeScan Plugin	https://jen	A-JEN-CODE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Storage of Sensitive Information			stores credentials unencrypted in its global configuration file on the Jenkins master where they can be viewed by users with access to the master file system. **CVE ID : CVE-2019-10423**	kins.io/security/advisory/2019-09-25/#SECURITY-1551	141019/189
eloyente					
Cleartext Storage of Sensitive Information	25-09-2019	2.1	Jenkins elOyente Plugin stores credentials unencrypted in its global configuration file on the Jenkins master where they can be viewed by users with access to the master file system. **CVE ID : CVE-2019-10424**	https://jenkins.io/security/advisory/2019-09-25/#SECURITY-1561	A-JEN-ELOY-141019/190
google_calendar					
Cleartext Storage of Sensitive Information	25-09-2019	4	Jenkins Google Calendar Plugin stores credentials unencrypted in job config.xml files on the Jenkins master where they can be viewed by users with Extended Read permission, or access to the master file system. **CVE ID : CVE-2019-10425**	https://jenkins.io/security/advisory/2019-09-25/#SECURITY-1572	A-JEN-GOOG-141019/191
gem_publisher					
Cleartext Storage of Sensitive Information	25-09-2019	2.1	Jenkins Gem Publisher Plugin stores credentials unencrypted in its global configuration file on the Jenkins master where they can be viewed by users with access to the master file system.	https://jenkins.io/security/advisory/2019-09-25/#SECURITY-1573	A-JEN-GEM_-141019/192

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10426		
gitlab_logo					
Cleartext Storage of Sensitive Information	25-09-2019	2.1	Jenkins GitLab Logo Plugin stores credentials unencrypted in its global configuration file on the Jenkins master where they can be viewed by users with access to the master file system. **CVE ID : CVE-2019-10429**	https://jenkins.io/security/advisory/2019-09-25/#SECURITY-1575	A-JEN-GITL-141019/193
neuvector_vulnerability_scanner					
Cleartext Storage of Sensitive Information	25-09-2019	2.1	Jenkins NeuVector Vulnerability Scanner Plugin 1.5 and earlier stored credentials unencrypted in its global configuration file on the Jenkins master where they could be viewed by users with access to the master file system. **CVE ID : CVE-2019-10430**	https://jenkins.io/security/advisory/2019-09-25/#SECURITY-1504	A-JEN-NEUV-141019/194
aqua_microscanner					
Cleartext Transmission of Sensitive Information	25-09-2019	5	Jenkins Aqua MicroScanner Plugin 1.0.7 and earlier transmitted configured credentials in plain text as part of the global Jenkins configuration form, potentially resulting in their exposure. **CVE ID : CVE-2019-10427**	https://jenkins.io/security/advisory/2019-09-25/#SECURITY-1507	A-JEN-AQUA-141019/195
Joomla					
joomla!					
Improper Neutralization of Input	24-09-2019	4.3	In Joomla! 3.x before 3.9.12, inadequate escaping allowed XSS attacks using the logo	https://developer.joomla.org/secur	A-JOO-JOOM-141019/196

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			parameter of the default templates. **CVE ID : CVE-2019-16725**	ity-centre/791-20190901-core-xss-in-logo-parameter-of-default-templates.html	
joyplus_project					
joyplus					
Improper Input Validation	21-09-2019	6.4	joyplus-cms 1.6.0 allows reinstallation if the install/ URI remains available. **CVE ID : CVE-2019-16655**	N/A	A-JOY-JOYP-141019/197
Improper Input Validation	21-09-2019	7.5	joyplus-cms 1.6.0 allows remote attackers to execute arbitrary PHP code via /install by placing the code in the name of an object in the database. **CVE ID : CVE-2019-16656**	N/A	A-JOY-JOYP-141019/198
Cross-Site Request Forgery (CSRF)	21-09-2019	6.8	joyplus-cms 1.6.0 has admin_ajax.php?action=save xml&tab=vodplay CSRF. **CVE ID : CVE-2019-16660**	N/A	A-JOY-JOYP-141019/199
kkcms_project					
kkcms					
Cross-Site Request Forgery (CSRF)	23-09-2019	6.8	kkcms v1.3 has a CSRF vulnerablity that can add an user account via admin/cms_user_add.php. **CVE ID : CVE-2019-16706**	N/A	A-KKC-KKCM-141019/200
Improper Neutralizatio n of Input During Web	27-09-2019	4.3	kkcms 1.3 has jx.php?url= XSS. **CVE ID : CVE-2019-16923**	N/A	A-KKC-KKCM-141019/201

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')					
layerbb					
layerbb					
Cross-Site Request Forgery (CSRF)	19-09-2019	6.8	LayerBB before 1.1.4 has multiple CSRF issues, as demonstrated by changing the System Settings via admin/general.php. **CVE ID : CVE-2019-16531**	N/A	A-LAY-LAYE-141019/202
Lenovo					
system_update					
Improper Input Validation	26-09-2019	7.8	A denial of service vulnerability was reported in Lenovo System Update versions prior to 5.07.0088 that could allow configuration files to be written to non-standard locations. **CVE ID : CVE-2019-6175**	N/A	A-LEN-SYST-141019/203
Libav					
libav					
Improper Input Validation	19-09-2019	7.1	In Libav 12.3, a denial of service in the subtitle decoder allows attackers to hog the CPU via a crafted video file in Matroska format, because srt_to_ass in libavcodec/srtdec.c has a complex format argument to sscanf. **CVE ID : CVE-2019-9717**	N/A	A-LIB-LIBA-141019/204
Buffer Copy without	19-09-2019	6.8	A stack-based buffer overflow in the subtitle	N/A	A-LIB-LIBA-141019/205

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			decoder in Libav 12.3 allows attackers to corrupt the stack via a crafted video file in Matroska format, because srt_to_ass in libavcodec/srtdec.c misuses snprintf. **CVE ID : CVE-2019-9719**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-09-2019	7.1	A stack-based buffer overflow in the subtitle decoder in Libav 12.3 allows attackers to corrupt the stack via a crafted video file in Matroska format, because srt_to_ass in libavcodec/srtdec.c misuses snprintf. **CVE ID : CVE-2019-9720**	N/A	A-LIB-LIBA-141019/206
libgcrypt20_project					
libgcrypt20					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	25-09-2019	6.8	It was discovered that there was a ECDSA timing attack in the libgcrypt20 cryptographic library. Version affected: 1.8.4-5, 1.7.6-2+deb9u3, and 1.6.3-2+deb8u4. Versions fixed: 1.8.5-2 and 1.6.3-2+deb8u7. **CVE ID : CVE-2019-13627**	N/A	A-LIB-LIBG-141019/207
Libming					
libming					
Out-of-bounds Read	23-09-2019	6.4	Ming (aka libming) 0.4.8 has an out of bounds read vulnerability in the function OpCode() in the decompile.c file in libutil.a. **CVE ID : CVE-2019-16705**	N/A	A-LIB-LIBM-141019/208

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
libwav_project					
libwav					
NULL Pointer Dereference	16-09-2019	4.3	marc-q libwav through 2019-08-15 has a NULL pointer dereference in gain_file() at wav_gain.c. **CVE ID : CVE-2019-16348**	N/A	A-LIB-LIBW-141019/209
linea_project					
linea					
Double Free	25-09-2019	7.5	An issue was discovered in the linea crate through 0.9.4 for Rust. There is double free in the Matrix::zip_elements method. **CVE ID : CVE-2019-16880**	https://rustsec.org/advisories/RUSTSEC-2019-0021.html	A-LIN-LINE-141019/210
Linecorp					
line					
Integer Overflow or Wraparound	19-09-2019	6.8	Integer overflow vulnerability in LINE(Android) from 4.4.0 to the version before 9.15.1 allows remote attackers to cause a denial of service (DoS) condition or execute arbitrary code via a specially crafted image. **CVE ID : CVE-2019-6010**	N/A	A-LIN-LINE-141019/211
Linuxfoundation					
runc					
Incorrect Authorization	25-09-2019	5	runc through 1.0.0-rc8, as used in Docker through 19.03.2-ce and other products, allows AppArmor restriction bypass because libcontainer/rootfs_linux.go incorrectly checks mount targets, and thus a malicious	N/A	A-LIN-RUNC-141019/212

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Docker image can mount over a /proc directory. **CVE ID : CVE-2019-16884**		
Linux-nfs					
nfs-utils					
Improper Privilege Management	19-09-2019	10	The nfs-utils package in SUSE Linux Enterprise Server 12 before and including version 1.3.0-34.18.1 and in SUSE Linux Enterprise Server 15 before and including version 2.1.1-6.10.2 the directory /var/lib/nfs is owned by statd:nogroup. This directory contains files owned and managed by root. If statd is compromised, it can therefore trick processes running with root privileges into creating/overwriting files anywhere on the system if fs.protected_symlinks is not set **CVE ID : CVE-2019-3689**	https://bugzilla.suse.com/show_bug.cgi?id=1150733	A-LIN-NFS--141019/213
Logmein					
lastpass					
Insufficiently Protected Credentials	16-09-2019	5.8	LogMeIn LastPass before 4.33.0 allows attackers to construct a crafted web site that captures the credentials for a victim's account on a previously visited web site, because do_popupregister can be bypassed via clickjacking. **CVE ID : CVE-2019-16371**	N/A	A-LOG-LAST-141019/214
makandra					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
consul					
Incorrect Authorization	23-09-2019	7.5	The makandra consul gem through 1.0.2 for Ruby has Incorrect Access Control. **CVE ID : CVE-2019-16377**	N/A	A-MAK-CONS-141019/215
Mediawiki					
mediawiki					
Information Exposure	25-09-2019	5	In MediaWiki through 1.33.0, Special:Redirect allows information disclosure of suppressed usernames via a User ID Lookup. **CVE ID : CVE-2019-16738**	N/A	A-MED-MEDI-141019/216
Microfocus					
service_manager					
Incorrect Authorization	18-09-2019	6.5	Allow changes to some table by non-SysAdmin in Micro Focus Service Manager product versions 9.30, 9.31, 9.32, 9.33, 9.34, 9.35, 9.40, 9.41, 9.50, 9.51, 9.52, 9.60, 9.61, 9.62. This vulnerability could be exploited to allow unauthorized access and modification of data. **CVE ID : CVE-2019-11661**	https://softwaresupport.softwaregrp.com/doc/KM03518316	A-MIC-SERV-141019/217
Information Exposure Through an Error Message	18-09-2019	4	Class and method names in error message in Micro Focus Service Manager product versions 9.30, 9.31, 9.32, 9.33, 9.34, 9.35, 9.40, 9.41, 9.50, 9.51, 9.52, 9.60, 9.61, 9.62. This vulnerability could be exploited in some special cases to allow information exposure through an error message.	https://softwaresupport.softwaregrp.com/doc/KM03518316	A-MIC-SERV-141019/218

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-11662		
Insufficiently Protected Credentials	18-09-2019	4	Clear text credentials are used to access managers app in Tomcat in Micro Focus Service Manager product versions 9.30, 9.31, 9.32, 9.33, 9.34, 9.35, 9.40, 9.41, 9.50, 9.51, 9.52, 9.60, 9.61, 9.62. The vulnerability could be exploited to allow sensitive data exposure. **CVE ID : CVE-2019-11663**	https://softwaresupport.softwaregrp.com/doc/KM03518316	A-MIC-SERV-141019/219
Insufficiently Protected Credentials	18-09-2019	4	Clear text password in browser in Micro Focus Service Manager product versions 9.30, 9.31, 9.32, 9.33, 9.34, 9.35, 9.40, 9.41, 9.50, 9.51, 9.52, 9.60, 9.61, 9.62. The vulnerability could be exploited to allow sensitive data exposure. **CVE ID : CVE-2019-11664**	https://softwaresupport.softwaregrp.com/doc/KM03518316	A-MIC-SERV-141019/220
Information Exposure	17-09-2019	5	Data exposure in Micro Focus Service Manager product versions 9.30, 9.31, 9.32, 9.33, 9.34, 9.35, 9.40, 9.41, 9.50, 9.51, 9.52, 9.60, 9.61, 9.62. The vulnerability could be exploited to allow sensitive data exposure. **CVE ID : CVE-2019-11665**	https://softwaresupport.softwaregrp.com/doc/KM03518316	A-MIC-SERV-141019/221
Deserialization of Untrusted Data	17-09-2019	6.8	Insecure deserialization of untrusted data in Micro Focus Service Manager product versions 9.30, 9.31, 9.32, 9.33, 9.34, 9.35, 9.40, 9.41, 9.50, 9.51, 9.52, 9.60, 9.61, 9.62. The vulnerability could be exploited to allow	https://softwaresupport.softwaregrp.com/doc/KM03518316	A-MIC-SERV-141019/222

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			insecure deserialization of untrusted data. **CVE ID : CVE-2019-11666**		
Information Exposure	17-09-2019	5	Unauthorized access to contact information in Micro Focus Service Manager, versions 9.41, 9.50, 9.51, 9.52, 9.60, 9.61, 9.62. The vulnerability could be exploited to allow unauthorized access to private data. **CVE ID : CVE-2019-11667**	https://softwaresupport.softwaregrp.com/doc/KM03517346	A-MIC-SERV-141019/223
Microsoft					
forefront_endpoint_protection_2010					
Improper Input Validation	23-09-2019	5	A denial of service vulnerability exists when Microsoft Defender improperly handles files, aka 'Microsoft Defender Denial of Service Vulnerability'. **CVE ID : CVE-2019-1255**	N/A	A-MIC-FORE-141019/224
security_essentials					
Improper Input Validation	23-09-2019	5	A denial of service vulnerability exists when Microsoft Defender improperly handles files, aka 'Microsoft Defender Denial of Service Vulnerability'. **CVE ID : CVE-2019-1255**	N/A	A-MIC-SECU-141019/225
system_center_endpoint_protection					
Improper Input Validation	23-09-2019	5	A denial of service vulnerability exists when Microsoft Defender improperly handles files, aka 'Microsoft Defender Denial of Service Vulnerability'.	N/A	A-MIC-SYST-141019/226

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-1255		
system_center_endpoint_protection_2012					
Improper Input Validation	23-09-2019	5	A denial of service vulnerability exists when Microsoft Defender improperly handles files, aka 'Microsoft Defender Denial of Service Vulnerability'. **CVE ID : CVE-2019-1255**	N/A	A-MIC-SYST-141019/227
windows_defender					
Improper Input Validation	23-09-2019	5	A denial of service vulnerability exists when Microsoft Defender improperly handles files, aka 'Microsoft Defender Denial of Service Vulnerability'. **CVE ID : CVE-2019-1255**	N/A	A-MIC-WIND-141019/228
internet_explorer					
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-09-2019	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1221. **CVE ID : CVE-2019-1367**	N/A	A-MIC-INTE-141019/229
moddable					
moddable					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-09-2019	7.5	In XS 9.0.0 in Moddable SDK OS180329, there is a heap-based buffer overflow in fxBeginHost in xsAPI.c when called from fxRunDefine in xsRun.c, as demonstrated by crafted JavaScript code to	N/A	A-MOD-MODD-141019/230

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			xst. **CVE ID : CVE-2019-16366**		
xs					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-09-2019	7.5	In XS 9.0.0 in Moddable SDK OS180329, there is a heap-based buffer overflow in fxBeginHost in xsAPI.c when called from fxRunDefine in xsRun.c, as demonstrated by crafted JavaScript code to xst. **CVE ID : CVE-2019-16366**	N/A	A-MOD-XS-141019/231
mz-automation					
libiec61850					
Use After Free	19-09-2019	5	libIEC61850 through 1.3.3 has a use-after-free in MmsServer_waitReady in mms/iso_mms/server/mms_server.c, as demonstrated by server_example_goose. **CVE ID : CVE-2019-16510**	N/A	A-MZ--LIBI-141019/232
Netapp					
ontap_select_deploy_administration_utility					
Improper Input Validation	24-09-2019	7.5	ONTAP Select Deploy administration utility versions 2.12 & 2.12.1 ship with an HTTP service bound to the network allowing unauthenticated remote attackers to perform administrative actions. **CVE ID : CVE-2019-5504**	N/A	A-NET-ONTA-141019/233
Insufficiently Protected Credentials	24-09-2019	5	ONTAP Select Deploy administration utility versions 2.2 through 2.12.1 transmit credentials in plaintext.	N/A	A-NET-ONTA-141019/234

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-5505		
Netgate					
Pfsense					
Cross-Site Request Forgery (CSRF)	26-09-2019	6.8	diag_command.php in pfSense 2.4.4-p3 allows CSRF via the txtCommand or txtRecallBuffer field, as demonstrated by executing OS commands. This occurs because csrf_callback() produces a "CSRF token expired" error and a Try Again button when a CSRF token is missing. **CVE ID : CVE-2019-16667**	N/A	A-NET-PFSE-141019/235
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	25-09-2019	9	pfSense through 2.3.4 through 2.4.4-p3 allows Remote Code Injection via a methodCall XML document with a pfsense.exec_php call containing shell metacharacters in a parameter value. **CVE ID : CVE-2019-16701**	N/A	A-NET-PFSE-141019/236
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-09-2019	4.3	An XSS issue was discovered in pfSense through 2.4.4-p3. In services_captiveportal_mac.php, the username and delmac parameters are displayed without sanitization. **CVE ID : CVE-2019-16914**	N/A	A-NET-PFSE-141019/237
Improper Input Validation	26-09-2019	7.5	An issue was discovered in pfSense through 2.4.4-p3. widgets/widgets/picture.widget.php uses the widgetkey parameter directly without	N/A	A-NET-PFSE-141019/238

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sanitization (e.g., a basename call) for a pathname to file_get_contents or file_put_contents. **CVE ID : CVE-2019-16915**		
netskope					
netskope					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	26-09-2019	7.2	The Netskope client service, v57 before 57.2.0.219 and v60 before 60.2.0.214, running with NT\SYSTEM privilege, accepts network connections from localhost. The connection handling function in this service suffers from a stack based buffer overflow in "doHandshakefromServer" function. Local users can use this vulnerability to trigger a crash of the service and potentially cause additional impact on the system. **CVE ID : CVE-2019-10882**	https://support.netskope.com/hc/en-us/articles/360014589894-Netskope-Client	A-NET-NETS-141019/239
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-09-2019	7.2	The Netskope client service, v57 before 57.2.0.219 and v60 before 60.2.0.214, running with NT\SYSTEM privilege, accepts network connections from localhost. The connection handling function in this service suffers from command injection vulnerability. Local users can use this vulnerability to execute code with NT\SYSTEM privilege. **CVE ID : CVE-2019-12091**	https://support.netskope.com/hc/en-us/articles/360014589894-Netskope-Client	A-NET-NETS-141019/240

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
netty					
netty					
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	26-09-2019	5	Netty before 4.1.42.Final mishandles whitespace before the colon in HTTP headers (such as a "Transfer-Encoding : chunked" line), which leads to HTTP request smuggling. **CVE ID : CVE-2019-16869**	N/A	A-NET-NETT-141019/241
ngiflib_project					
ngiflib					
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-09-2019	6.8	ngiflib 0.4 has a heap-based buffer overflow in WritePixel() in ngiflib.c when called from DecodeGifImg, because deinterlacing for small pictures is mishandled. **CVE ID : CVE-2019-16346**	N/A	A-NGI-NGIF-141019/242
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-09-2019	6.8	ngiflib 0.4 has a heap-based buffer overflow in WritePixels() in ngiflib.c when called from DecodeGifImg, because deinterlacing for small pictures is mishandled. **CVE ID : CVE-2019-16347**	N/A	A-NGI-NGIF-141019/243
Open-emr					
openemr					
Improper Neutralization of Input During Web Page Generation ('Cross-site	16-09-2019	4.3	OpenEMR v5.0.1-6 allows XSS. **CVE ID : CVE-2019-8368**	N/A	A-OPE-OPEN-141019/244

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')					
Improper Control of Generation of Code ('Code Injection')	16-09-2019	9	OpenEMR v5.0.1-6 allows code execution. **CVE ID : CVE-2019-8371**	N/A	A-OPE-OPEN-141019/245
pac4j					
pac4j					
Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)	23-09-2019	4	The SAML identifier generated within SAML2Utils.java was found to make use of the apache commons-lang3 RandomStringUtils class which makes them predictable due to RandomStringUtils PRNG's algorithm not being cryptographically strong. This issue only affects the 3.X release of pac4j-saml. **CVE ID : CVE-2019-10755**	N/A	A-PAC-PAC4-141019/246
pagekit					
pagekit					
Information Exposure Through Discrepancy	21-09-2019	5	The Reset Password feature in Pagekit 1.0.17 gives a different response depending on whether the e-mail address of a valid user account is entered, which might make it easier for attackers to enumerate accounts. **CVE ID : CVE-2019-16669**	N/A	A-PAG-PAGE-141019/247
pam-python_project					
pam-python					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	24-09-2019	7.2	pam-python before 1.0.7-1 has an issue in regard to the default environment variable handling of Python, which could allow for local root escalation in certain PAM setups. **CVE ID : CVE-2019-16729**	N/A	A-PAM-PAM--141019/248
Phpbb					
phpbb					
Cross-Site Request Forgery (CSRF)	27-09-2019	4.3	phpBB version 3.2.7 allows the stealing of an Administration Control Panel session id by leveraging CSRF in the Remote Avatar feature. The CSRF Token Hijacking leads to stored XSS **CVE ID : CVE-2019-13376**	N/A	A-PHP-PHPB-141019/249
Phpipam					
phpipam					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-09-2019	7.5	phpIPAM 1.4 allows SQL injection via the app/admin/custom-fields/filter-result.php table parameter when action=add is used. **CVE ID : CVE-2019-16692**	N/A	A-PHP-PHPI-141019/250
Improper Neutralization of Special Elements used in an SQL Command ('SQL	22-09-2019	7.5	phpIPAM 1.4 allows SQL injection via the app/admin/custom-fields/order.php table parameter when action=add is used. **CVE ID : CVE-2019-16693**	N/A	A-PHP-PHPI-141019/251

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-09-2019	7.5	phpIPAM 1.4 allows SQL injection via the app/admin/custom-fields/edit-result.php table parameter when action=add is used. **CVE ID : CVE-2019-16694**	N/A	A-PHP-PHPI-141019/252
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-09-2019	7.5	phpIPAM 1.4 allows SQL injection via the app/admin/custom-fields/filter.php table parameter when action=add is used. **CVE ID : CVE-2019-16695**	N/A	A-PHP-PHPI-141019/253
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-09-2019	7.5	phpIPAM 1.4 allows SQL injection via the app/admin/custom-fields/edit.php table parameter when action=add is used. **CVE ID : CVE-2019-16696**	N/A	A-PHP-PHPI-141019/254
phpmywind					
phpmywind					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-09-2019	4.3	admin/infolist_add.php in PHPMyWind 5.6 has stored XSS. **CVE ID : CVE-2019-16703**	N/A	A-PHP-PHPM-141019/255
Improper	23-09-2019	3.5	admin/infoclass_update.php	N/A	A-PHP-PHPM-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			in PHPMyWind 5.6 has stored XSS. **CVE ID : CVE-2019-16704**		141019/256
pivotal_software					
pivotal_application_service					
Improper Privilege Management	20-09-2019	6.5	Pivotal Apps Manager, included in Pivotal Application Service versions 2.3.x prior to 2.3.18, 2.4.x prior to 2.4.14, 2.5.x prior to 2.5.10, and 2.6.x prior to 2.6.5, contains an invitations microservice which allows users to invite others to their organizations. A remote authenticated user can gain additional privileges by inviting themselves to spaces that they should not have access to. **CVE ID : CVE-2019-11280**	https://pivotal.io/security/cve-2019-11280	A-PIV-PIVO-141019/257
plutinosoft					
platinum					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	26-09-2019	5	Platinum UPnP SDK 1.2.0 allows Directory Traversal in Core/PltHttpServer.cpp because it checks for /.. where it should be checking for ../ instead. **CVE ID : CVE-2019-16903**	N/A	A-PLU-PLAT-141019/258
portaudio-rs_project					
portaudio-rs					
Use After	25-09-2019	7.5	An issue was discovered in	https://rust	A-POR-PORT-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Free			the portaudio-rs crate through 0.3.1 for Rust. There is a use-after-free with resultant arbitrary code execution because of a lack of unwind safety in stream_callback and stream_finished_callback. **CVE ID : CVE-2019-16881**	sec.org/advisories/RUSTSEC-2019-0022.html	141019/259
prise					
adas					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-09-2019	4.3	An issue was discovered in PRiSE adAS 1.7.0. The OPENSSO module does not properly escape output on error, leading to reflected XSS. **CVE ID : CVE-2019-14911**	N/A	A-PRI-ADAS-141019/260
URL Redirection to Untrusted Site ('Open Redirect')	20-09-2019	5.8	An issue was discovered in PRiSE adAS 1.7.0. The OPENSSO module does not properly check the goto parameter, leading to an open redirect that leaks the session cookie. **CVE ID : CVE-2019-14912**	N/A	A-PRI-ADAS-141019/261
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-09-2019	3.5	An issue was discovered in PRiSE adAS 1.7.0. Log data are not properly escaped, leading to persistent XSS in the administration panel. **CVE ID : CVE-2019-14913**	N/A	A-PRI-ADAS-141019/262
Improper Limitation of a Pathname to a	20-09-2019	7.5	An issue was discovered in PRiSE adAS 1.7.0. The path is not properly escaped in the medatadata_del method,	N/A	A-PRI-ADAS-141019/263

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restricted Directory ('Path Traversal')			leading to an arbitrary file read and deletion via Directory Traversal. **CVE ID : CVE-2019-14914**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-09-2019	4.3	An issue was discovered in PRiSE adAS 1.7.0. Certificate data are not properly escaped. This leads to XSS when submitting a rogue certificate. **CVE ID : CVE-2019-14915**	N/A	A-PRI-ADAS-141019/264
Unrestricted Upload of File with Dangerous Type	20-09-2019	4	An issue was discovered in PRiSE adAS 1.7.0. A file's format is not properly checked, leading to an unrestricted file upload. **CVE ID : CVE-2019-14916**	N/A	A-PRI-ADAS-141019/265
Insufficiently Protected Credentials	20-09-2019	5	An issue was discovered in PRiSE adAS 1.7.0. The current database password is embedded in the change password form. **CVE ID : CVE-2019-15085**	N/A	A-PRI-ADAS-141019/266
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-09-2019	4.3	An issue was discovered in PRiSE adAS 1.7.0. The newentityID parameter is not properly escaped, leading to a reflected XSS in the error message. **CVE ID : CVE-2019-15086**	N/A	A-PRI-ADAS-141019/267
Missing Authorization	20-09-2019	6.5	An issue was discovered in PRiSE adAS 1.7.0. An authenticated user can change the function used to hash passwords to any function, leading to remote	N/A	A-PRI-ADAS-141019/268

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code execution. **CVE ID : CVE-2019-15087**		
Incorrect Type Conversion or Cast	20-09-2019	7.5	An issue was discovered in PRiSE adAS 1.7.0. Password hashes are compared using the equality operator. Thus, under specific circumstances, it is possible to bypass login authentication. **CVE ID : CVE-2019-15088**	N/A	A-PRI-ADAS-141019/269
Cross-Site Request Forgery (CSRF)	20-09-2019	6.8	An issue was discovered in PRiSE adAS 1.7.0. Forms have no CSRF protection, letting an attacker execute actions as the administrator. **CVE ID : CVE-2019-15089**	N/A	A-PRI-ADAS-141019/270
publisure					
publisure					
Unrestricted Upload of File with Dangerous Type	18-09-2019	6.5	An issue was discovered in the secure portal in Publisure 2.1.2. Once successfully authenticated as an administrator, one is able to inject arbitrary PHP code by using the adminCons.php form. The code is then stored in the E:\PUBLISURE\webservice\webpages\AdminDir\Templates\ folder even if removed from the adminCons.php view (i.e., the rogue PHP file can be hidden). **CVE ID : CVE-2019-14252**	N/A	A-PUB-PUBL-141019/271
Incorrect Authorization	18-09-2019	6.4	An issue was discovered in servletcontroller in the secure portal in Publisure	N/A	A-PUB-PUBL-141019/272

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.1.2. One can bypass authentication and perform a query on PHP forms within the /AdminDir folder that should be restricted. **CVE ID : CVE-2019-14253**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-09-2019	7.5	An issue was discovered in the secure portal in Publisure 2.1.2. Because SQL queries are not well sanitized, there are multiple SQL injections in userAccFunctions.php functions. Using this, an attacker can access passwords and/or grant access to the user account "user" in order to become "Administrator" (for example). **CVE ID : CVE-2019-14254**	N/A	A-PUB-PUBL-141019/273
Pydio					
pydio					
Information Exposure Through an Error Message	19-09-2019	5	Pydio 6.0.8 mishandles error reporting when a directory allows unauthenticated uploads, and the remote-upload option is used with the http://localhost:22 URL. The attacker can obtain sensitive information such as the name of the user who created that directory and other internal server information. **CVE ID : CVE-2019-15032**	N/A	A-PYD-PYDI-141019/274
Server-Side Request Forgery	19-09-2019	4	Pydio 6.0.8 allows Authenticated SSRF during a Remote Link Feature	N/A	A-PYD-PYDI-141019/275

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
(SSRF)			download. An attacker can specify an intranet address in the file parameter to index.php, when sending a file to a remote server, as demonstrated by the file=http%3A%2F%2F192.168.1.2 substring. **CVE ID : CVE-2019-15033**		
Qemu					
qemu					
Loop with Unreachable Exit Condition ('Infinite Loop')	24-09-2019	5	In QEMU 1:4.1-1, 1:2.1+dfsg-12+deb8u6, 1:2.8+dfsg-6+deb9u8, 1:3.1+dfsg-8~deb10u1, 1:3.1+dfsg-8+deb10u2, and 1:2.1+dfsg-12+deb8u12 (fixed), when executing script in lsi_execute_script(), the LSI scsi adapter emulator advances 's->dsp' index to read next opcode. This can lead to an infinite loop if the next opcode is empty. Move the existing loop exit after 10k iterations so that it covers no-op opcodes as well. **CVE ID : CVE-2019-12068**	N/A	A-QEM-QEMU-141019/276
Radare					
radare2					
Improper Neutralization of Special Elements used in an OS Command ('OS Command	23-09-2019	6.8	In radare2 before 3.9.0, a command injection vulnerability exists in bin_symbols() in libr/core/cbin.c. By using a crafted executable file, it's possible to execute arbitrary shell commands with the	N/A	A-RAD-RADA-141019/277

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			permissions of the victim. This vulnerability is due to an insufficient fix for CVE-2019-14745 and improper handling of symbol names embedded in executables. **CVE ID : CVE-2019-16718**		
redlion					
crimson					
Use of Hard-coded Credentials	23-09-2019	4.3	Red Lion Controls Crimson, version 3.0 and prior and version 3.1 prior to release 3112.00, uses a hard-coded password to encrypt protected files in transit and at rest, which may allow an attacker to access configuration files. **CVE ID : CVE-2019-10990**	N/A	A-RED-CRIM-141019/278
Use After Free	23-09-2019	6.8	Red Lion Controls Crimson, version 3.0 and prior and version 3.1 prior to release 3112.00, allow multiple vulnerabilities to be exploited when a valid user opens a specially crafted, malicious input file that can reference memory after it has been freed. **CVE ID : CVE-2019-10996**	N/A	A-RED-CRIM-141019/279
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-09-2019	6.8	Red Lion Controls Crimson, version 3.0 and prior and version 3.1 prior to release 3112.00, allow multiple vulnerabilities to be exploited when a valid user opens a specially crafted, malicious input file that operates outside of the	N/A	A-RED-CRIM-141019/280

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			designated memory area. **CVE ID : CVE-2019-10978**		
Access of Uninitialized Pointer	23-09-2019	6.8	Red Lion Controls Crimson, version 3.0 and prior and version 3.1 prior to release 3112.00, allow multiple vulnerabilities to be exploited when a valid user opens a specially crafted, malicious input file that causes the program to mishandle pointers. **CVE ID : CVE-2019-10984**	N/A	A-RED-CRIM-141019/281
redmineup					
crm					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-09-2019	4.3	The CRM Plugin before 4.2.4 for Redmine allows XSS via crafted vCard data. **CVE ID : CVE-2019-15950**	N/A	A-RED-CRM-141019/282
reputeinfosystems					
arforms					
Improper Input Validation	27-09-2019	6.4	In the ARforms plugin 3.7.1 for WordPress, arf_delete_file in arformcontroller.php allows unauthenticated deletion of an arbitrary file by supplying the full pathname. **CVE ID : CVE-2019-16902**	N/A	A-REP-ARFO-141019/283
riot-os					
riot					
NULL Pointer	24-09-2019	5	RIOT 2019.07 contains a NULL pointer dereference in	N/A	A-RIO-RIOT-141019/284

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Dereference			the MQTT-SN implementation (asymcute), potentially allowing an attacker to crash a network node running RIOT. This requires spoofing an MQTT server response. To do so, the attacker needs to know the MQTT MsgID of a pending MQTT protocol message and the ephemeral port used by RIOT's MQTT implementation. Additionally, the server IP address is required for spoofing the packet. **CVE ID : CVE-2019-16754**		
Rockwellautomation					
arena_simulation_software					
Access of Uninitialized Pointer	24-09-2019	6.8	In Rockwell Automation Arena Simulation Software Cat. 9502-Ax, Versions 16.00.00 and earlier, a maliciously crafted Arena file opened by an unsuspecting user may result in the use of a pointer that has not been initialized. **CVE ID : CVE-2019-13527**	N/A	A-ROC-AREN-141019/285
RSA					
bsafe_cert-j					
Improper Verification of Cryptographic Signature	18-09-2019	4.3	RSA BSAFE Crypto-J versions prior to 6.2.5 are vulnerable to an Improper Verification of Cryptographic Signature vulnerability. A malicious remote attacker could potentially exploit this vulnerability to coerce two	N/A	A-RSA-BSAF-141019/286

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			parties into computing the same predictable shared key. **CVE ID : CVE-2019-3738**		
Information Exposure Through Discrepancy	18-09-2019	4.3	RSA BSAFE Crypto-J versions prior to 6.2.5 are vulnerable to Information Exposure Through Timing Discrepancy vulnerabilities during ECDSA key generation. A malicious remote attacker could potentially exploit those vulnerabilities to recover ECDSA keys. **CVE ID : CVE-2019-3739**	N/A	A-RSA-BSAF-141019/287
Information Exposure	18-09-2019	4.3	RSA BSAFE Crypto-J versions prior to 6.2.5 are vulnerable to an Information Exposure Through Timing Discrepancy vulnerabilities during DSA key generation. A malicious remote attacker could potentially exploit those vulnerabilities to recover DSA keys. **CVE ID : CVE-2019-3740**	N/A	A-RSA-BSAF-141019/288
bsafe_ssl-j					
Improper Verification of Cryptographic Signature	18-09-2019	4.3	RSA BSAFE Crypto-J versions prior to 6.2.5 are vulnerable to an Improper Verification of Cryptographic Signature vulnerability. A malicious remote attacker could potentially exploit this vulnerability to coerce two parties into computing the same predictable shared key. **CVE ID : CVE-2019-3738**	N/A	A-RSA-BSAF-141019/289
Information	18-09-2019	4.3	RSA BSAFE Crypto-J versions	N/A	A-RSA-BSAF-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure Through Discrepancy			prior to 6.2.5 are vulnerable to Information Exposure Through Timing Discrepancy vulnerabilities during ECDSA key generation. A malicious remote attacker could potentially exploit those vulnerabilities to recover ECDSA keys. **CVE ID : CVE-2019-3739**		141019/290
Information Exposure	18-09-2019	4.3	RSA BSAFE Crypto-J versions prior to 6.2.5 are vulnerable to an Information Exposure Through Timing Discrepancy vulnerabilities during DSA key generation. A malicious remote attacker could potentially exploit those vulnerabilities to recover DSA keys. **CVE ID : CVE-2019-3740**	N/A	A-RSA-BSAF-141019/291
archer					
Information Exposure	18-09-2019	4	RSA Archer, versions prior to 6.6 P3 (6.6.0.3), contain an information disclosure vulnerability. Information relating to the backend database gets disclosed to low-privileged RSA Archer users' UI under certain error conditions. **CVE ID : CVE-2019-3756**	N/A	A-RSA-ARCH-141019/292
Improper Authentication	18-09-2019	7.5	RSA Archer, versions prior to 6.6 P2 (6.6.0.2), contain an improper authentication vulnerability. The vulnerability allows sysadmins to create user accounts with insufficient	N/A	A-RSA-ARCH-141019/293

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			credentials. Unauthenticated attackers could gain unauthorized access to the system using those accounts. **CVE ID : CVE-2019-3758**		
sahipro					
sahi_pro					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-09-2019	5	Within Sahi Pro 8.0.0, an attacker can send a specially crafted URL to include any victim files on the system via the script parameter on the Script_view page. This will result in file disclosure (i.e., being able to pull any file from the remote victim application). This can be used to steal and obtain sensitive config and other files. This can result in complete compromise of the application. The script parameter is vulnerable to directory traversal and both local and remote file inclusion. **CVE ID : CVE-2019-13063**	N/A	A-SAH-SAHI-141019/294
Schneider-electric					
somachine_hvac					
Untrusted Search Path	17-09-2019	6.8	A CWE-426: Untrusted Search Path vulnerability exists in SoMachine HVAC v2.4.1 and earlier versions, which could cause arbitrary code execution on the system running SoMachine HVAC when a malicious DLL library is loaded by the	https://www.schneider-electric.com/en/download/document/SEVD-2019-225-04/	A-SCH-SOMA-141019/295

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			product. **CVE ID : CVE-2019-6826**		
Silverstripe					
silverstripe					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-09-2019	3.5	In SilverStripe asset-admin 4.0, there is XSS in file titles managed through the CMS. **CVE ID : CVE-2019-14272**	https://www.silverstripe.org/download/security-releases/CVE-2019-14272	A-SIL-SILV-141019/296
Files or Directories Accessible to External Parties	26-09-2019	5	In SilverStripe assets 4.0, there is broken access control on files. **CVE ID : CVE-2019-14273**	https://www.silverstripe.org/download/security-releases/CVE-2019-14273	A-SIL-SILV-141019/297
Session Fixation	25-09-2019	3.7	SilverStripe through 4.3.3 allows session fixation in the "change password" form. **CVE ID : CVE-2019-12203**	https://www.silverstripe.org/download/security-releases/CVE-2019-12203	A-SIL-SILV-141019/298
Improper Privilege Management	25-09-2019	7.5	In SilverStripe through 4.3.3, a missing warning about leaving install.php in a public webroot can lead to unauthenticated admin access. **CVE ID : CVE-2019-12204**	https://www.silverstripe.org/download/security-releases/CVE-2019-12204	A-SIL-SILV-141019/299
Improper Neutralization of Input	25-09-2019	4.3	SilverStripe through 4.3.3 has Flash Clipboard	https://www.silverstripe.org/dow	A-SIL-SILV-141019/300

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			Reflected XSS. **CVE ID : CVE-2019-12205**	nload/security-releases/CVE-2019-12205	
Information Exposure	25-09-2019	5	SilverStripe through 4.3.3 has incorrect access control for protected files uploaded via Upload::loadIntoFile(). An attacker may be able to guess a filename in silverstripe/assets via the AssetControlExtension. **CVE ID : CVE-2019-12245**	https://www.silverstripe.org/download/security-releases/CVE-2019-12245	A-SIL-SILV-141019/301
Improper Privilege Management	26-09-2019	4	In SilverStripe through 4.3.3, there is access escalation for CMS users with limited access through permission cache pollution. **CVE ID : CVE-2019-12617**	https://www.silverstripe.org/download/security-releases/CVE-2019-12617	A-SIL-SILV-141019/302
Spip					
spip					
Incorrect Authorization	17-09-2019	4	SPIP before 3.1.11 and 3.2 before 3.2.5 allows authenticated visitors to modify any published content and execute other modifications in the database. This is related to ecrire/inc/meta.php and ecrire/inc/securiser_action.php. **CVE ID : CVE-2019-16391**	N/A	A-SPI-SPIP-141019/303
Improper Neutralization of Input During Web	17-09-2019	4.3	SPIP before 3.1.11 and 3.2 before 3.2.5 allows prive/formulaires/login.php	N/A	A-SPI-SPIP-141019/304

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')			XSS via error messages. **CVE ID : CVE-2019-16392**		
URL Redirection to Untrusted Site ('Open Redirect')	17-09-2019	5.8	SPIP before 3.1.11 and 3.2 before 3.2.5 mishandles redirect URLs in ecrire/inc/headers.php with a %0D, %0A, or %20 character. **CVE ID : CVE-2019-16393**	N/A	A-SPI-SPIP-141019/305
Information Exposure	17-09-2019	5	SPIP before 3.1.11 and 3.2 before 3.2.5 provides different error messages from the password-reminder page depending on whether an e-mail address exists, which might help attackers to enumerate subscribers. **CVE ID : CVE-2019-16394**	N/A	A-SPI-SPIP-141019/306
string-interner_project					
string-interner					
Use After Free	25-09-2019	5	An issue was discovered in the string-interner crate before 0.7.1 for Rust. It allows attackers to read from memory locations associated with dangling pointers, because of a cloning flaw. **CVE ID : CVE-2019-16882**	https://rustsec.org/advisories/RUSTSEC-2019-0023.html	A-STR-STRI-141019/307
suricata-ids					
suricata					
Out-of-bounds Read	24-09-2019	6.4	An issue was discovered in app-layer-ssl.c in Suricata 4.1.4. Upon receiving a corrupted SSLv3 (TLS 1.2) packet, the parser function	N/A	A-SUR-SURI-141019/308

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			TLSDecodeHSHelloExtensions tries to access a memory region that is not allocated, because the expected length of HSHelloExtensions does not match the real length of the HSHelloExtensions part of the packet. **CVE ID : CVE-2019-15699**		
Out-of-bounds Read	24-09-2019	6.4	An issue was discovered in Suricata 4.1.4. By sending multiple fragmented IPv4 packets, the function Defrag4Reassemble in defrag.c tries to access a memory region that is not allocated, because of a lack of header_len checking. **CVE ID : CVE-2019-16410**	N/A	A-SUR-SURI-141019/309
Out-of-bounds Read	24-09-2019	7.5	An issue was discovered in Suricata 4.1.4. By sending multiple IPv4 packets that have invalid IPv4Options, the function IPV4OptValidateTimestamp in decode-ipv4.c tries to access a memory region that is not allocated. There is a check for o->len < 5 (corresponding to 2 bytes of header and 3 bytes of data). Then, "flag = *(o->data + 3)" places one beyond the 3 bytes, because the code should have been "flag = *(o->data + 1)" instead. **CVE ID : CVE-2019-16411**	N/A	A-SUR-SURI-141019/310
Symantec					
norton_password_manager					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	17-09-2019	2.1	Norton Password Manager, prior to 6.5.0.2104, may be susceptible to an information disclosure issue, which is a type of vulnerability whereby there is an unintentional disclosure of information to an actor that is not explicitly authorized to have access to that information. **CVE ID : CVE-2019-12755**	https://support.symantec.com/us/en/article.SYMSA1493.html	A-SYM-NORT-141019/311
Teampass					
teampass					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-09-2019	3.5	TeamPass 2.1.27.36 allows Stored XSS by setting a crafted password for an item in a common available folder or sharing the item with an admin. (The crafted password is exploitable when viewing the change history of the item or tapping on the item.) **CVE ID : CVE-2019-16904**	N/A	A-TEA-TEAM-141019/312
terrasoft					
bpm_online_crm_system_sdk					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-09-2019	7.5	A SQL injection vulnerability in the method Terrasoft.Core.DB.Column.Const() in Terrasoft Bpm'online CRM-System SDK 7.13 allows attackers to execute arbitrary SQL commands via the value parameter. **CVE ID : CVE-2019-15301**	N/A	A-TER-BPM_-141019/313
thinksaas					

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
thinksaas					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-09-2019	3.5	An issue was discovered in ThinkSAAS 2.91. There is XSS via the index.php?app=group&ac=create&ts=do groupname parameter. **CVE ID : CVE-2019-16664**	N/A	A-THI-THIN-141019/314
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-09-2019	4.3	An issue was discovered in ThinkSAAS 2.91. There is XSS via the content to the index.php?app=group&ac=comment&ts=do&js=1 URI, as demonstrated by a crafted SVG document in the SRC attribute of an EMBED element. **CVE ID : CVE-2019-16665**	N/A	A-THI-THIN-141019/315
Tibco					
enterprise_runtime_for_r					
Improper Input Validation	18-09-2019	10	The server component of TIBCO Software Inc.'s TIBCO Enterprise Runtime for R - Server Edition, and TIBCO Spotfire Analytics Platform for AWS Marketplace contains a vulnerability that theoretically allows an unauthenticated user to bypass access controls and remotely execute code using the operating system account hosting the affected component. This issue affects: TIBCO Enterprise Runtime for R - Server Edition versions 1.2.0 and below, and TIBCO Spotfire	https://www.tibco.com/support/advisories/2019/09/tibco-security-advisory-september-17-2019-tibco-enterprise-runtime-for-r-server-2019-11210	A-TIB-ENTE-141019/316

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Analytics Platform for AWS Marketplace versions 10.4.0 and 10.5.0. **CVE ID : CVE-2019-11210**		
Improper Input Validation	18-09-2019	9	The server component of TIBCO Software Inc.'s TIBCO Enterprise Runtime for R - Server Edition, and TIBCO Spotfire Analytics Platform for AWS Marketplace contains a vulnerability that theoretically allows an authenticated user to trigger remote code execution in certain circumstances. When the affected component runs with the containerized TERR service on Linux the host can theoretically be tricked into running malicious code. This issue affects: TIBCO Enterprise Runtime for R - Server Edition version 1.2.0 and below, and TIBCO Spotfire Analytics Platform for AWS Marketplace 10.4.0; 10.5.0. **CVE ID : CVE-2019-11211**	https://www.tibco.com/support/advisories/2019/09/tibco-security-advisory-september-17-2019-tibco-enterprise-runtime-for-r-server-2019-11211	A-TIB-ENTE-141019/317
spotfire_analytics_platform_for_aws					
Improper Input Validation	18-09-2019	10	The server component of TIBCO Software Inc.'s TIBCO Enterprise Runtime for R - Server Edition, and TIBCO Spotfire Analytics Platform for AWS Marketplace contains a vulnerability that theoretically allows an unauthenticated user to bypass access controls and remotely execute code using	https://www.tibco.com/support/advisories/2019/09/tibco-security-advisory-september-17-2019-tibco-enterprise-	A-TIB-SPOT-141019/318

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the operating system account hosting the affected component. This issue affects: TIBCO Enterprise Runtime for R - Server Edition versions 1.2.0 and below, and TIBCO Spotfire Analytics Platform for AWS Marketplace versions 10.4.0 and 10.5.0. **CVE ID : CVE-2019-11210**	runtime-for-r-server-2019-11210	
Improper Input Validation	18-09-2019	9	The server component of TIBCO Software Inc.'s TIBCO Enterprise Runtime for R - Server Edition, and TIBCO Spotfire Analytics Platform for AWS Marketplace contains a vulnerability that theoretically allows an authenticated user to trigger remote code execution in certain circumstances. When the affected component runs with the containerized TERR service on Linux the host can theoretically be tricked into running malicious code. This issue affects: TIBCO Enterprise Runtime for R - Server Edition version 1.2.0 and below, and TIBCO Spotfire Analytics Platform for AWS Marketplace 10.4.0; 10.5.0. **CVE ID : CVE-2019-11211**	https://www.tibco.com/support/advisories/2019/09/tibco-security-advisory-september-17-2019-tibco-enterprise-runtime-for-r-server-2019-11211	A-TIB-SPOT-141019/319
totaldefense					
anti-virus					
Improper Privilege	24-09-2019	4.6	In Total Defense Anti-virus 9.0.0.773, insecure access	N/A	A-TOT-ANTI-141019/320

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			control for the directory %PROGRAMDATA%\TotalDefense\Consumer\ISS\9\ used by ccschedulersvc.exe allows local attackers to hijack dotnetproxy.exe, which leads to privilege escalation when the ccSchedulerSVC service runs the executable. **CVE ID : CVE-2019-13355**		
Improper Privilege Management	24-09-2019	4.6	In Total Defense Anti-virus 9.0.0.773, insecure access control for the directory %PROGRAMDATA%\TotalDefense\Consumer\ISS\9\bd\TDUpdate2\ used by AMRT.exe allows local attackers to hijack bdcore.dll, which leads to privilege escalation when the AMRT service loads the DLL. **CVE ID : CVE-2019-13356**	N/A	A-TOT-ANTI-141019/321
Untrusted Search Path	24-09-2019	4.6	In Total Defense Anti-virus 9.0.0.773, resource acquisition from the untrusted search path C:\ used by caschelp.exe allows local attackers to hijack ccGUIFrm.dll, which leads to code execution. SYSTEM-level code execution can be achieved when the ccSchedulerSVC service runs the affected executable. **CVE ID : CVE-2019-13357**	N/A	A-TOT-ANTI-141019/322
traveloka					
traveloka					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-09-2019	2.6	The Traveloka application 3.14.0 for Android exports com.traveloka.android.activity.common.WebViewActivity, leading to the opening of arbitrary URLs, which can inject deceptive content into the UI. (When in physical possession of the device, opening local files is also possible.) NOTE: As of 2019-09-23, the vendor has not agreed that this issue has serious impact. The vendor states that the issue is not critical because it does not allow Elevation of Privilege, Sensitive Data Leakage, or any critical unauthorized activity from a malicious user. The vendor also states that a victim must first install a malicious APK to their application. **CVE ID : CVE-2019-16681**	N/A	A-TRA-TRAV-141019/323
trusteddomain					
opendmarc					
Authentication Bypass by Spoofing	17-09-2019	7.5	OpenDMARC through 1.3.2 and 1.4.x through 1.4.0-Beta1 is prone to a signature-bypass vulnerability with multiple From: addresses, which might affect applications that consider a domain name to be relevant to the origin of an e-mail message. **CVE ID : CVE-2019-16378**	N/A	A-TRU-OPEN-141019/324
tuzicms					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
tuzicms					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-09-2019	7.5	App\Home\Controller\ZhuantiController.class.php in TuziCMS 2.0.6 has SQL injection via the index.php/Zhuanti/group?id = substring. **CVE ID : CVE-2019-16644**	N/A	A-TUZ-TUZI-141019/325
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-09-2019	4.3	TuziCMS 2.0.6 has XSS via the PATH_INFO to a group URI, as demonstrated by index.php/article/group/id/2/. **CVE ID : CVE-2019-16657**	N/A	A-TUZ-TUZI-141019/326
Cross-Site Request Forgery (CSRF)	21-09-2019	6.8	TuziCMS 2.0.6 has index.php/manage/notice/do_add CSRF. **CVE ID : CVE-2019-16658**	N/A	A-TUZ-TUZI-141019/327
Cross-Site Request Forgery (CSRF)	21-09-2019	6.8	TuziCMS 2.0.6 has index.php/manage/link/do_add CSRF. **CVE ID : CVE-2019-16659**	N/A	A-TUZ-TUZI-141019/328
Upredsun					
file_sharing_wizard					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	24-09-2019	7.5	File Sharing Wizard 1.5.0 allows a remote attacker to obtain arbitrary code execution by exploiting a Structured Exception Handler (SEH) based buffer overflow in an HTTP POST parameter, a similar issue to CVE-2010-2330 and CVE-2010-2331.	N/A	A-UPR-FILE-141019/329

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-16724		
Valvesoftware					
counter-strike:_global_offensive					
Improper Input Validation	19-09-2019	6.8	vphysics.dll in Counter-Strike: Global Offensive before 1.37.1.1 allows remote attackers to achieve code execution or denial of service by creating a gaming server and inviting a victim to this server, because a crafted map is mishandled during a memset call. **CVE ID : CVE-2019-15943**	https://github.com/bi7s/CVE/blob/master/CVE-2019-15943/README.md	A-VAL-COUN-141019/330
Vbulletin					
vbulletin					
Improper Input Validation	24-09-2019	7.5	vBulletin 5.x through 5.5.4 allows remote command execution via the widgetConfig[code] parameter in an ajax/render/widget_php routestring request. **CVE ID : CVE-2019-16759**	N/A	A-VBU-VBUL-141019/331
Vmware					
workstation					
Out-of-bounds Read	20-09-2019	5.5	VMware ESXi (6.7 before ESXi670-201904101-SG and 6.5 before ESXi650-201903001), Workstation (15.x before 15.0.3 and 14.x before 14.1.6) and Fusion (11.x before 11.0.3 and 10.x before 10.1.6) contain an out-of-bounds read vulnerability in the pixel shader functionality. Successful exploitation of	https://www.vmware.com/security/advisories/VMSA-2019-0012.html	A-VMW-WORK-141019/332

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			this issue may lead to information disclosure or may allow attackers with normal user privileges to create a denial-of-service condition on the host. Exploitation of this issue require an attacker to have access to a virtual machine with 3D graphics enabled. It is not enabled by default on ESXi and is enabled by default on Workstation and Fusion. **CVE ID : CVE-2019-5521**		
fusion					
Out-of-bounds Read	20-09-2019	5.5	VMware ESXi (6.7 before ESXi670-201904101-SG and 6.5 before ESXi650-201903001), Workstation (15.x before 15.0.3 and 14.x before 14.1.6) and Fusion (11.x before 11.0.3 and 10.x before 10.1.6) contain an out-of-bounds read vulnerability in the pixel shader functionality. Successful exploitation of this issue may lead to information disclosure or may allow attackers with normal user privileges to create a denial-of-service condition on the host. Exploitation of this issue require an attacker to have access to a virtual machine with 3D graphics enabled. It is not enabled by default on ESXi and is enabled by	https://www.vmware.com/security/advisories/VMSA-2019-0012.html	A-VMW-FUSI-141019/333

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			default on Workstation and Fusion. **CVE ID : CVE-2019-5521**		
vcenter_server					
Insufficient Session Expiration	18-09-2019	5.8	VMware vSphere ESXi (6.7 prior to ESXi670-201810101-SG, 6.5 prior to ESXi650-201811102-SG, and 6.0 prior to ESXi600-201807103-SG) and VMware vCenter Server (6.7 prior to 6.7 U1b, 6.5 prior to 6.5 U2b, and 6.0 prior to 6.0 U3j) contain an information disclosure vulnerability in clients arising from insufficient session expiration. An attacker with physical access or an ability to mimic a websocket connection to a user?s browser may be able to obtain control of a VM Console after the user has logged out or their session has timed out. **CVE ID : CVE-2019-5531**	http://www.vmware.com/security/advisories/VMSA-2019-0013.html	A-VMW-VCEN-141019/334
Insufficiently Protected Credentials	18-09-2019	4	VMware vCenter Server (6.7.x prior to 6.7 U3, 6.5 prior to 6.5 U3 and 6.0 prior to 6.0 U3j) contains an information disclosure vulnerability due to the logging of credentials in plain-text for virtual machines deployed through OVF. A malicious user with access to the log files containing vCenter OVF-properties of a virtual	https://www.vmware.com/security/advisories/VMSA-2019-0013.html	A-VMW-VCEN-141019/335

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			machine deployed from an OVF may be able to view the credentials used to deploy the OVF (typically the root account of the virtual machine). **CVE ID : CVE-2019-5532**		
Insufficiently Protected Credentials	18-09-2019	4	VMware vCenter Server (6.7.x prior to 6.7 U3, 6.5 prior to 6.5 U3 and 6.0 prior to 6.0 U3j) contains an information disclosure vulnerability where Virtual Machines deployed from an OVF could expose login information via the virtual machine's vAppConfig properties. A malicious actor with access to query the vAppConfig properties of a virtual machine deployed from an OVF may be able to view the credentials used to deploy the OVF (typically the root account of the virtual machine). **CVE ID : CVE-2019-5534**	https://www.vmware.com/security/advisories/VMSA-2019-0013.html	A-VMW-VCEN-141019/336
vsphere_esxi					
Insufficient Session Expiration	18-09-2019	5.8	VMware vSphere ESXi (6.7 prior to ESXi670-201810101-SG, 6.5 prior to ESXi650-201811102-SG, and 6.0 prior to ESXi600-201807103-SG) and VMware vCenter Server (6.7 prior to 6.7 U1b, 6.5 prior to 6.5 U2b, and 6.0 prior to 6.0 U3j) contain an information disclosure vulnerability in clients arising from	http://www.vmware.com/security/advisories/VMSA-2019-0013.html	A-VMW-VSPH-141019/337

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			insufficient session expiration. An attacker with physical access or an ability to mimic a websocket connection to a user?s browser may be able to obtain control of a VM Console after the user has logged out or their session has timed out. **CVE ID : CVE-2019-5531**		
Webkul					
bagisto					
Incorrect Authorizatio n	18-09-2019	6.5	In Webkul Bagisto before 0.1.5, the functionalities for customers to change their own values (such as address, review, orders, etc.) can also be manipulated by other customers. **CVE ID : CVE-2019-16403**	N/A	A-WEB-BAGI-141019/338
Wolfssl					
wolfssl					
Out-of-bounds Read	24-09-2019	7.5	In wolfSSL through 4.1.0, there is a missing sanity check of memory accesses in parsing ASN.1 certificate data while handshaking. Specifically, there is a one-byte heap-based buffer over-read in CheckCertSignature_ex in wolfcrypt/src/asn.c. **CVE ID : CVE-2019-16748**	N/A	A-WOL-WOLF-141019/339
wtcms_project					
wtcms					
Cross-Site	23-09-2019	4.3	WTCMS 1.0 allows	N/A	A-WTC-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Request Forgery (CSRF)			index.php?g=admin&m=index&a=index CSRF with resultant XSS. **CVE ID : CVE-2019-16719**		WTCM-141019/340
yejiao					
tuzicms					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-09-2019	7.5	App\Mobile\Controller\ZhuantiController.class.php in TuziCMS 2.0.6 has SQL injection via the index.php/Mobile/Zhuanti/group?id= substring. **CVE ID : CVE-2019-16642**	N/A	A-YEJ-TUZI-141019/341
Yzmcms					
Yzmcms					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	26-09-2019	5.8	An HTTP Host header injection vulnerability exists in YzmCMS V5.3. A malicious user can poison a web cache or trigger redirections. **CVE ID : CVE-2019-16532**	N/A	A-YZM-YZMC-141019/342
Cross-Site Request Forgery (CSRF)	21-09-2019	4.3	admin/urlrule/add.html in YzmCMS 5.3 allows CSRF with a resultant denial of service by adding a superseding route. **CVE ID : CVE-2019-16678**	N/A	A-YZM-YZMC-141019/343
zrlog					
zrlog					
Improper Neutralization of Input	20-09-2019	3.5	An issue was discovered in ZrLog 2.1.1. There is a Stored XSS vulnerability in	N/A	A-ZRL-ZRLO-141019/344

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			the article_edit area. **CVE ID : CVE-2019-16643**		
Zulip					
zulip_server					
Uncontrolled Resource Consumption	18-09-2019	4	The Markdown parser in Zulip server before 2.0.5 used a regular expression vulnerable to exponential backtracking. A user who is logged into the server could send a crafted message causing the server to spend an effectively arbitrary amount of CPU time and stall the processing of future messages. **CVE ID : CVE-2019-16215**	https://github.com/zulip/zulip/commit/5797f013b3be450c146a4141514bda525f2f1b51	A-ZUL-ZULI-141019/345
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-09-2019	3.5	Zulip server before 2.0.5 incompletely validated the MIME types of uploaded files. A user who is logged into the server could upload files of certain types to mount a stored cross-site scripting attack on other logged-in users. On a Zulip server using the default local uploads backend, the attack is only effective against browsers lacking support for Content-Security-Policy such as Internet Explorer 11. On a Zulip server using the S3 uploads backend, the attack is confined to the origin of the configured S3 uploads hostname and cannot reach	https://github.com/zulip/zulip/commit/1195841dfb9aa26b3b0dabc6f05d72e4af25be3e	A-ZUL-ZULI-141019/346

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the Zulip server itself. **CVE ID : CVE-2019-16216**		
zzzcms					
zzzphp					
Unrestricted Upload of File with Dangerous Type	23-09-2019	5	ZZZCMS zzzphp v1.7.2 does not properly restrict file upload in plugins/ueditor/php/controller.php?upfolder=news&action=catchimage, as demonstrated by uploading a .htaccess or .php5 file. **CVE ID : CVE-2019-16720**	N/A	A-ZZZ-ZZZP-141019/347
Improper Input Validation	23-09-2019	7.5	ZZZCMS zzzphp v1.7.2 has an insufficient protection mechanism against PHP Code Execution, because passthru bypasses an str_ireplace operation. **CVE ID : CVE-2019-16722**	N/A	A-ZZZ-ZZZP-141019/348
Operating System					
Canonical					
ubuntu_linux					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-09-2019	7.2	A buffer overflow flaw was found, in versions from 2.6.34 to 5.2.x, in the way Linux kernel's vhost functionality that translates virtqueue buffers to IOVs, logged the buffer descriptors during migration. A privileged guest user able to pass descriptors with invalid length to the host when migration is underway, could use this flaw to increase their privileges on	N/A	O-CAN-UBUN-141019/349

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the host. **CVE ID : CVE-2019-14835**		
Cisco					
nx-os					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	25-09-2019	7.2	A vulnerability in a CLI command related to the virtualization manager (VMAN) in Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying Linux operating system with root privileges. The vulnerability is due to insufficient validation of arguments passed to a specific VMAN CLI command on an affected device. An attacker could exploit this vulnerability by including malicious input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system with root privileges, which may lead to complete system compromise. An attacker would need valid administrator credentials to exploit this vulnerability. **CVE ID : CVE-2019-12717**	N/A	O-CIS-NX-O-141019/350
ios_xr					
Improper Neutralization of Special	25-09-2019	7.2	A vulnerability in a CLI command related to the virtualization manager	N/A	O-CIS-IOS_-141019/351

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			(VMAN) in Cisco IOS XR Software for Cisco ASR 9000 Series Aggregation Services Routers could allow an authenticated, local attacker to execute arbitrary commands on the underlying Linux operating system with root privileges. The vulnerability is due to insufficient validation of arguments passed to a specific VMAN CLI command on an affected device. An attacker who has valid administrator access to an affected device could exploit this vulnerability by including malicious input as the argument of an affected command. A successful exploit could allow the attacker to run arbitrary commands on the underlying operating system with root privileges, which may lead to complete system compromise. **CVE ID : CVE-2019-12709**		
ios					
Inadequate Encryption Strength	25-09-2019	5.8	A vulnerability in the HTTP client feature of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to read and modify data that should normally have been sent via an encrypted channel. The vulnerability is due to TCP port information not being	N/A	O-CIS-IOS-141019/352

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			considered when matching new requests to existing, persistent HTTP connections. An attacker could exploit this vulnerability by acting as a man-in-the-middle and then reading and/or modifying data that should normally have been sent through an encrypted channel. **CVE ID : CVE-2019-12665**		
Improper Link Resolution Before File Access ('Link Following')	25-09-2019	7.2	A vulnerability in the filesystem of Cisco IOS XE Software could allow an authenticated, local attacker with physical access to an affected device to execute arbitrary code on the underlying operating system (OS) with root privileges. The vulnerability is due to insufficient file location validation. An attacker could exploit this vulnerability by placing code in a specific format on a USB device and inserting it into an affected Cisco device. A successful exploit could allow the attacker to execute the code with root privileges on the underlying OS of the affected device. **CVE ID : CVE-2019-12672**	N/A	O-CIS-IOS-141019/353
hyperflex_hx220c_af_m5_firmware					
Insufficient Verification of Data	18-09-2019	5	A vulnerability in the statistics collection service of Cisco HyperFlex Software could allow an	N/A	O-CIS-HYPE-141019/354

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Authenticity			unauthenticated, remote attacker to inject arbitrary values on an affected device. The vulnerability is due to insufficient authentication for the statistics collection service. An attacker could exploit this vulnerability by sending properly formatted data values to the statistics collection service of an affected device. A successful exploit could allow the attacker to cause the web interface statistics view to present invalid data to users. **CVE ID : CVE-2019-12620**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-09-2019	4.3	A vulnerability in the web-based interface of Cisco HyperFlex Software could allow an unauthenticated, remote attacker to execute a cross-frame scripting (XFS) attack on an affected device. This vulnerability is due to insufficient HTML iframe protection. An attacker could exploit this vulnerability by directing a user to an attacker-controlled web page that contains a malicious HTML iframe. A successful exploit could allow the attacker to conduct clickjacking or other clientside browser attacks. **CVE ID : CVE-2019-1975**	N/A	O-CIS-HYPE-141019/355
hyperflex_hx220c_edge_m5_firmware					
Insufficient Verification	18-09-2019	5	A vulnerability in the statistics collection service	N/A	O-CIS-HYPE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Data Authenticity			of Cisco HyperFlex Software could allow an unauthenticated, remote attacker to inject arbitrary values on an affected device. The vulnerability is due to insufficient authentication for the statistics collection service. An attacker could exploit this vulnerability by sending properly formatted data values to the statistics collection service of an affected device. A successful exploit could allow the attacker to cause the web interface statistics view to present invalid data to users. **CVE ID : CVE-2019-12620**		141019/356
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-09-2019	4.3	A vulnerability in the web-based interface of Cisco HyperFlex Software could allow an unauthenticated, remote attacker to execute a cross-frame scripting (XFS) attack on an affected device. This vulnerability is due to insufficient HTML iframe protection. An attacker could exploit this vulnerability by directing a user to an attacker-controlled web page that contains a malicious HTML iframe. A successful exploit could allow the attacker to conduct clickjacking or other clientside browser attacks. **CVE ID : CVE-2019-1975**	N/A	O-CIS-HYPE-141019/357
hyperflex_hx220c_m5_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Insufficient Verification of Data Authenticity	18-09-2019	5	A vulnerability in the statistics collection service of Cisco HyperFlex Software could allow an unauthenticated, remote attacker to inject arbitrary values on an affected device. The vulnerability is due to insufficient authentication for the statistics collection service. An attacker could exploit this vulnerability by sending properly formatted data values to the statistics collection service of an affected device. A successful exploit could allow the attacker to cause the web interface statistics view to present invalid data to users. **CVE ID : CVE-2019-12620**	N/A	O-CIS-HYPE-141019/358
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-09-2019	4.3	A vulnerability in the web-based interface of Cisco HyperFlex Software could allow an unauthenticated, remote attacker to execute a cross-frame scripting (XFS) attack on an affected device. This vulnerability is due to insufficient HTML iframe protection. An attacker could exploit this vulnerability by directing a user to an attacker-controlled web page that contains a malicious HTML iframe. A successful exploit could allow the attacker to conduct clickjacking or other clientside browser attacks.	N/A	O-CIS-HYPE-141019/359

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-1975		
hyperflex_hx240c_af_m5_firmware					
Insufficient Verification of Data Authenticity	18-09-2019	5	A vulnerability in the statistics collection service of Cisco HyperFlex Software could allow an unauthenticated, remote attacker to inject arbitrary values on an affected device. The vulnerability is due to insufficient authentication for the statistics collection service. An attacker could exploit this vulnerability by sending properly formatted data values to the statistics collection service of an affected device. A successful exploit could allow the attacker to cause the web interface statistics view to present invalid data to users. **CVE ID : CVE-2019-12620**	N/A	O-CIS-HYPE-141019/360
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-09-2019	4.3	A vulnerability in the web-based interface of Cisco HyperFlex Software could allow an unauthenticated, remote attacker to execute a cross-frame scripting (XFS) attack on an affected device. This vulnerability is due to insufficient HTML iframe protection. An attacker could exploit this vulnerability by directing a user to an attacker-controlled web page that contains a malicious HTML iframe. A successful exploit could allow the attacker to conduct	N/A	O-CIS-HYPE-141019/361

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			clickjacking or other clientside browser attacks. **CVE ID : CVE-2019-1975**		
hyperflex_hx240c_m5_firmware					
Insufficient Verification of Data Authenticity	18-09-2019	5	A vulnerability in the statistics collection service of Cisco HyperFlex Software could allow an unauthenticated, remote attacker to inject arbitrary values on an affected device. The vulnerability is due to insufficient authentication for the statistics collection service. An attacker could exploit this vulnerability by sending properly formatted data values to the statistics collection service of an affected device. A successful exploit could allow the attacker to cause the web interface statistics view to present invalid data to users. **CVE ID : CVE-2019-12620**	N/A	O-CIS-HYPE-141019/362
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-09-2019	4.3	A vulnerability in the web-based interface of Cisco HyperFlex Software could allow an unauthenticated, remote attacker to execute a cross-frame scripting (XFS) attack on an affected device. This vulnerability is due to insufficient HTML iframe protection. An attacker could exploit this vulnerability by directing a user to an attacker-controlled web page that contains a malicious HTML iframe. A	N/A	O-CIS-HYPE-141019/363

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to conduct clickjacking or other clientside browser attacks. **CVE ID : CVE-2019-1975**		
Dlink					
dns-320_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	16-09-2019	10	The login_mgr.cgi script in D-Link DNS-320 through 2.05.B10 is vulnerable to remote command injection. **CVE ID : CVE-2019-16057**	N/A	O-DLI-DNS--141019/364
Draytek					
vigor2925_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-09-2019	4.3	On DrayTek Vigor2925 devices with firmware 3.8.4.3, Incorrect Access Control exists in loginset.htm, and can be used to trigger XSS. NOTE: this is an end-of-life product. This has been solved in v3.8.8.2 and later release firmware. **CVE ID : CVE-2019-16533**	N/A	O-DRA-VIGO-141019/365
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-09-2019	4.3	On DrayTek Vigor2925 devices with firmware 3.8.4.3, XSS exists via a crafted WAN name on the General Setup screen. NOTE: this is an end-of-life product. This has been solved in v3.8.8.2 and later release firmware	N/A	O-DRA-VIGO-141019/366

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-16534		
Fedoraproject					
fedora					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-09-2019	7.5	process_http_response in OpenConnect before 8.05 has a Buffer Overflow when a malicious server uses HTTP chunked encoding with crafted chunk sizes. **CVE ID : CVE-2019-16239**	N/A	O-FED-FEDO-141019/367
gigastone					
smart_battery_a4_firmware					
Improper Authentication	25-09-2019	10	A broken access control vulnerability in Smart Battery A4, a multifunctional portable charger, firmware version ?<= r1.7.9 allows an attacker to get/reset administrator's password without any authentication. **CVE ID : CVE-2019-15068**	https://www.twcert.org.tw/subpages/ServeThePublic/public_document_details.aspx?lang=en-US&id=45	O-GIG-SMAR-141019/368
Improper Authentication	25-09-2019	7.5	An unsafe authentication interface was discovered in Smart Battery A4, a multifunctional portable charger, firmware version ?<= r1.7.9 . An attacker can bypass authentication without modifying device file and gain web page management privilege. **CVE ID : CVE-2019-15069**	https://www.twcert.org.tw/subpages/ServeThePublic/public_document_details.aspx?lang=en-US&id=46	O-GIG-SMAR-141019/369
Google					
android					
Improper Initialization	27-09-2019	4.3	In libxaac there is a possible information disclosure due	N/A	O-GOO-ANDR-141019/370

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to uninitialized data. This could lead to information disclosure with no additional execution privileges needed. User interaction is needed for exploitation. Product: AndroidVersions: Android-10Android ID: A-113035086 **CVE ID : CVE-2019-2171**		
Missing Initialization of Resource	27-09-2019	4.3	In libavc there is a possible information disclosure due to uninitialized data. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation. Product: AndroidVersions: Android-10Android ID: A-112204376 **CVE ID : CVE-2019-9337**	N/A	O-GOO-ANDR-141019/371
Missing Initialization of Resource	27-09-2019	4.3	In libavc there is a possible information disclosure due to uninitialized data. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation. Product: AndroidVersions: Android-10Android ID: A-111762686 **CVE ID : CVE-2019-9338**	N/A	O-GOO-ANDR-141019/372
Out-of-bounds Read	27-09-2019	5	In Bluetooth, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional	N/A	O-GOO-ANDR-141019/373

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android-10Android ID: A-111214770 **CVE ID : CVE-2019-9341**		
Out-of-bounds Read	27-09-2019	5	In Bluetooth, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android-10Android ID: A-111214470 **CVE ID : CVE-2019-9342**	N/A	O-GOO-ANDR-141019/374
Out-of-bounds Read	27-09-2019	5	In Bluetooth, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android-10Android ID: A-112050983 **CVE ID : CVE-2019-9343**	N/A	O-GOO-ANDR-141019/375
Out-of-bounds Write	27-09-2019	6.8	In libstagefright, there is a possible out of bounds write due to a heap buffer overflow. This could lead to remote code execution with no additional execution	N/A	O-GOO-ANDR-141019/376

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is needed for exploitation. Product: AndroidVersions: Android-10Android ID: A-128433933 **CVE ID : CVE-2019-9346**		
Improper Input Validation	27-09-2019	7.1	In libstagefright, there is a possible resource exhaustion due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed. User interaction is needed for exploitation. Product: AndroidVersions: Android-10Android ID: A-128431761 **CVE ID : CVE-2019-9348**	N/A	O-GOO-ANDR-141019/377
Out-of-bounds Read	27-09-2019	4.3	In Bluetooth, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation. Product: AndroidVersions: Android-10Android ID: A-123024201 **CVE ID : CVE-2019-9353**	N/A	O-GOO-ANDR-141019/378
Out-of-bounds Read	27-09-2019	5	In Bluetooth, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	N/A	O-GOO-ANDR-141019/379

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Product: AndroidVersions: Android-10Android ID: A-115903122 **CVE ID : CVE-2019-9355**		
Improper Input Validation	27-09-2019	7.5	In Bluetooth, there is a possible deserialization error due to missing string validation. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android-10Android ID: A-109838537 **CVE ID : CVE-2019-9365**	N/A	O-GOO-ANDR-141019/380
Out-of-bounds Read	27-09-2019	5	In Bluetooth, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android-10Android ID: A-112106425 **CVE ID : CVE-2019-9367**	N/A	O-GOO-ANDR-141019/381
Out-of-bounds Read	27-09-2019	2.1	In Bluetooth, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android-	N/A	O-GOO-ANDR-141019/382

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			10Android ID: A-79883568 **CVE ID : CVE-2019-9368**		
Improper Input Validation	27-09-2019	7.1	In libskia, there is a possible crash due to a missing null check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is needed for exploitation. Product: AndroidVersions: Android-10Android ID: A-132782448 **CVE ID : CVE-2019-9372**	N/A	O-GOO-ANDR-141019/383
Out-of-bounds Read	27-09-2019	5	In Bluetooth, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android-10Android ID: A-117569833 **CVE ID : CVE-2019-9387**	N/A	O-GOO-ANDR-141019/384
Out-of-bounds Read	27-09-2019	5	In Bluetooth, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure in the Bluetooth service with no additional execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android-10Android ID: A-117567437	N/A	O-GOO-ANDR-141019/385

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-9388		
Out-of-bounds Read	27-09-2019	5	In Bluetooth, there is a possible out of bounds read due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android-10Android ID: A-117567058 **CVE ID : CVE-2019-9389**	N/A	O-GOO-ANDR-141019/386
Out-of-bounds Read	27-09-2019	5	In Bluetooth, there is a possible out of bounds read due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android-10Android ID: A-117551475 **CVE ID : CVE-2019-9390**	N/A	O-GOO-ANDR-141019/387
Inadequate Encryption Strength	27-09-2019	4.3	The Print Service is susceptible to man in the middle attacks due to improperly used crypto. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android-10Android ID: A-115635664 **CVE ID : CVE-2019-9399**	N/A	O-GOO-ANDR-141019/388
N/A	27-09-2019	4.3	In libavc there is a possible	N/A	O-GOO-ANDR-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information disclosure due to uninitialized data. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation. Product: AndroidVersions: Android-10Android ID: A-112380157 **CVE ID : CVE-2019-9408**		141019/389
N/A	27-09-2019	4.3	In libavc there is a possible information disclosure due to uninitialized data. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation. Product: AndroidVersions: Android-10Android ID: A-112204443 **CVE ID : CVE-2019-9410**	N/A	O-GOO-ANDR-141019/390
N/A	27-09-2019	4.3	In libavc there is a possible information disclosure due to uninitialized data. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation. Product: AndroidVersions: Android-10Android ID: A-112204845 **CVE ID : CVE-2019-9411**	N/A	O-GOO-ANDR-141019/391
Out-of-bounds Read	27-09-2019	5	In Bluetooth, there is a possible out of bounds read due to a missing bounds check. This could lead to	N/A	O-GOO-ANDR-141019/392

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android-10Android ID: A-111935831 **CVE ID : CVE-2019-9413**		
N/A	27-09-2019	4.3	In libstagefright there is a possible information disclosure due to uninitialized data. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation. Product: AndroidVersions: Android-10Android ID: A-111805098 **CVE ID : CVE-2019-9415**	N/A	O-GOO-ANDR-141019/393
N/A	27-09-2019	4.3	In libstagefright there is a possible information disclosure due to uninitialized data. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation. Product: AndroidVersions: Android-10Android ID: A-111804142 **CVE ID : CVE-2019-9416**	N/A	O-GOO-ANDR-141019/394
Out-of-bounds Read	27-09-2019	2.1	In Bluetooth, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution	N/A	O-GOO-ANDR-141019/395

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android-10Android ID: A-111450079 **CVE ID : CVE-2019-9417**		
Out-of-bounds Read	27-09-2019	5	In Bluetooth, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android-10Android ID: A-111407544 **CVE ID : CVE-2019-9419**	N/A	O-GOO-ANDR-141019/396
Out-of-bounds Read	27-09-2019	5	In Bluetooth, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android-10Android ID: A-111214766 **CVE ID : CVE-2019-9422**	N/A	O-GOO-ANDR-141019/397
Out-of-bounds Read	27-09-2019	5	In Bluetooth, there is a possible out of bounds read due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User	N/A	O-GOO-ANDR-141019/398

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interaction is not needed for exploitation. Product: AndroidVersions: Android-10Android ID: A-110846194 **CVE ID : CVE-2019-9425**		
Use After Free	27-09-2019	4	In Bluetooth, there is a possible out of bounds read due to a use after free. This could lead to remote information disclosure with heap information written to the log with System execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android-10Android ID: A-109755179 **CVE ID : CVE-2019-9431**	N/A	O-GOO-ANDR-141019/399
Out-of-bounds Read	27-09-2019	5	In Bluetooth, there is a possible out of bounds read due to improper input validation. This could lead to remote information disclosure in the Bluetooth server with no additional execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android-10Android ID: A-80546108 **CVE ID : CVE-2019-9432**	N/A	O-GOO-ANDR-141019/400
Improper Input Validation	27-09-2019	4.3	In libvpx, there is a possible information disclosure due to improper input validation. This could lead to remote information disclosure with no additional execution	N/A	O-GOO-ANDR-141019/401

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is needed for exploitation. Product: AndroidVersions: Android-10Android ID: A-80479354 **CVE ID : CVE-2019-9433**		
Out-of-bounds Read	27-09-2019	4	In Bluetooth, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with heap information written to the log with System execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android-10Android ID: A-80432895 **CVE ID : CVE-2019-9434**	N/A	O-GOO-ANDR-141019/402
Out-of-bounds Read	27-09-2019	2.1	In Bluetooth, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android-10Android ID: A-80146682 **CVE ID : CVE-2019-9435**	N/A	O-GOO-ANDR-141019/403
Out-of-bounds Read	27-09-2019	5	In Bluetooth, there is a possible out of bounds read due to an incorrect bounds check. This could lead to remote denial of service with no additional execution privileges needed. User	N/A	O-GOO-ANDR-141019/404

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interaction is not needed for exploitation. Product: AndroidVersions: Android-10Android ID: A-91544774 **CVE ID : CVE-2019-9462**		
Intel					
e5-4628l_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-E5-4-141019/405
e5-4657l_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-E5-4-141019/406
e7-2850_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-E7-2-141019/407
e7-2870_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-E7-2-141019/408
e7-2880_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-E7-2-141019/409
e7-2890_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-E7-2-141019/410
e7-4860_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	O-INT-E7-4-141019/411

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Condition')			**CVE ID : CVE-2019-11184**	00290.html	
e7-4870_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-E7-4-141019/412
e7-4880_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-E7-4-141019/413
e7-4890_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-E7-4-141019/414
e7-8850_firmware					
Concurrent Execution using Shared Resource with Improper	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial	https://www.intel.com/content/www/us/en/security-center/advi	O-INT-E7-8-141019/415

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Synchronization ('Race Condition')			information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	sory/intel-sa-00290.html	
e7-8857_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-E7-8-141019/416
e7-8895_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-E7-8-141019/417
e5-2623_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-E5-2-141019/418
e5-2628l_firmware					
Concurrent Execution using Shared	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation	https://www.intel.com/content/w	O-INT-E5-2-141019/419

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource with Improper Synchronization ('Race Condition')			and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	ww/us/en/security-center/advisory/intel-sa-00290.html	
e5-2630_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-E5-2-141019/420
e5-2630l_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-E5-2-141019/421
e5-2637_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-E5-2-141019/422
e5-2640_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-E5-2-141019/423
e5-2643_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-E5-2-141019/424
e5-2648l_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-E5-2-141019/425
e5-2650_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	O-INT-E5-2-141019/426

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Condition')			**CVE ID : CVE-2019-11184**	00290.html	
e5-2650l_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-E5-2-141019/427
e5-2658_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-E5-2-141019/428
e5-2660_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-E5-2-141019/429
e5-2667_firmware					
Concurrent Execution using Shared Resource with Improper	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial	https://www.intel.com/content/www/us/en/security-center/advi	O-INT-E5-2-141019/430

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Synchronization ('Race Condition')			information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	sory/intel-sa-00290.html	
e5-2670_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-E5-2-141019/431
e5-2680_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-E5-2-141019/432
e5-2683_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-E5-2-141019/433
e5-2687w_firmware					
Concurrent Execution using Shared	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation	https://www.intel.com/content/w	O-INT-E5-2-141019/434

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource with Improper Synchronization ('Race Condition')			and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	ww/us/en/security-center/advisory/intel-sa-00290.html	
e5-2690_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-E5-2-141019/435
e5-2695_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-E5-2-141019/436
e5-2697_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-E5-2-141019/437
e5-2698_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-E5-2-141019/438
e5-2699_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-E5-2-141019/439
e5-4610_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-E5-4-141019/440
e5-4620_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	O-INT-E5-4-141019/441

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Condition')			**CVE ID : CVE-2019-11184**	00290.html	
e5-4627_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-E5-4-141019/442
e5-4640_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-E5-4-141019/443
e5-4650_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-E5-4-141019/444
e5-4655_firmware					
Concurrent Execution using Shared Resource with Improper	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial	https://www.intel.com/content/www/us/en/security-center/advi	O-INT-E5-4-141019/445

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Synchronization ('Race Condition')			information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	sory/intel-sa-00290.html	
e5-4660_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-E5-4-141019/446
e5-4667_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-E5-4-141019/447
e5-4669_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-E5-4-141019/448
e7-4809_firmware					
Concurrent Execution using Shared	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation	https://www.intel.com/content/w	O-INT-E7-4-141019/449

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource with Improper Synchronization ('Race Condition')			and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	ww/us/en/security-center/advisory/intel-sa-00290.html	
e7-4820_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-E7-4-141019/450
e7-4830_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-E7-4-141019/451
e7-4850_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-E7-4-141019/452
e7-8870_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-E7-8-141019/453
e7-8880_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-E7-8-141019/454
e7-8880l_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-E7-8-141019/455
e7-8890_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	O-INT-E7-8-141019/456

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Condition')			**CVE ID : CVE-2019-11184**	00290.html	
e7-8891_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-E7-8-141019/457
e7-8893_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-E7-8-141019/458
3106_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-3106-141019/459
4109t_firmware					
Concurrent Execution using Shared Resource with Improper	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial	https://www.intel.com/content/www/us/en/security-center/advi	O-INT-4109-141019/460

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Synchronization ('Race Condition')			information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	sory/intel-sa-00290.html	
4110_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-4110-141019/461
4114t_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-4114-141019/462
4116_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-4116-141019/463
4116t_firmware					
Concurrent Execution using Shared	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation	https://www.intel.com/content/w	O-INT-4116-141019/464

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource with Improper Synchronization ('Race Condition')			and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	ww/us/en/security-center/advisory/intel-sa-00290.html	
5118_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-5118-141019/465
5119t_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-5119-141019/466
5120t_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-5120-141019/467
6126_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-6126-141019/468
6126t_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-6126-141019/469
6130_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-6130-141019/470
6130t_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	O-INT-6130-141019/471

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Condition')			**CVE ID : CVE-2019-11184**	00290.html	
6138_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-6138-141019/472
e5-2403_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-E5-2-141019/473
e5-2407_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-E5-2-141019/474
e5-2420_firmware					
Concurrent Execution using Shared Resource with Improper	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial	https://www.intel.com/content/www/us/en/security-center/advi	O-INT-E5-2-141019/475

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Synchronization ('Race Condition')			information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	sory/intel-sa-00290.html	
e5-2430_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-E5-2-141019/476
e5-2430l_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-E5-2-141019/477
e5-2440_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-E5-2-141019/478
e5-2450_firmware					
Concurrent Execution using Shared	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation	https://www.intel.com/content/w	O-INT-E5-2-141019/479

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource with Improper Synchronization ('Race Condition')			and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	ww/us/en/security-center/advisory/intel-sa-00290.html	
e5-2450l_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-E5-2-141019/480
e5-2470_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-E5-2-141019/481
e5-2697a_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-E5-2-141019/482
e5-2699a_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-E5-2-141019/483
e5-4603_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-E5-4-141019/484
e5-4607_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-E5-4-141019/485
e5-1620_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	O-INT-E5-1-141019/486

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Condition')			**CVE ID : CVE-2019-11184**	00290.html	
e5-1630_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-E5-1-141019/487
e5-1650_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-E5-1-141019/488
e5-1660_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-E5-1-141019/489
e5-1680_firmware					
Concurrent Execution using Shared Resource with Improper	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial	https://www.intel.com/content/www/us/en/security-center/advi	O-INT-E5-1-141019/490

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Synchronization ('Race Condition')			information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	sory/intel-sa-00290.html	
e5-2603_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-E5-2-141019/491
e5-2608l_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-E5-2-141019/492
e5-2609_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-E5-2-141019/493
e5-2618l_firmware					
Concurrent Execution using Shared	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation	https://www.intel.com/content/w	O-INT-E5-2-141019/494

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource with Improper Synchronization ('Race Condition')			and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	ww/us/en/security-center/advisory/intel-sa-00290.html	
e5-2620_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. **CVE ID : CVE-2019-11184**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html	O-INT-E5-2-141019/495
intenogroup					
eg200_firmware					
Information Exposure Through Discrepancy	16-09-2019	4.3	Inteno EG200 EG200-WU7P1U_ADAMO3.16.4-190226_1650 routers have a JUCI ACL misconfiguration that allows the "user" account to extract the 3DES key via JSON commands to ubus. The 3DES key is used to decrypt the provisioning file provided by Adamo Telecom on a public URL via cleartext HTTP. **CVE ID : CVE-2019-13140**	N/A	O-INT-EG20-141019/496
keeper					
k5_firmware					
Improper Input Validation	19-09-2019	7.2	On Keeper K5 20.1.0.25 and 20.1.0.63 devices, remote code execution can occur by inserting an SD card containing a file named	N/A	O-KEE-K5_F-141019/497

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			zskj_script_run.sh that executes a reverse shell. **CVE ID : CVE-2019-16398**		
Linux					
linux_kernel					
Information Exposure	23-09-2019	5	In the Linux kernel before 5.2.14, rds6_inc_info_copy in net/rds/recv.c allows attackers to obtain sensitive information from kernel stack memory because tos and flags fields are not initialized. **CVE ID : CVE-2019-16714**	N/A	O-LIN-LINU-141019/498
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	24-09-2019	7.5	An issue was discovered in net/wireless/nl80211.c in the Linux kernel through 5.2.17. It does not check the length of variable elements in a beacon head, leading to a buffer overflow. **CVE ID : CVE-2019-16746**	N/A	O-LIN-LINU-141019/499
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-09-2019	7.2	There is heap-based buffer overflow in Linux kernel, all versions up to, excluding 5.3, in the marvell wifi chip driver in Linux kernel, that allows local users to cause a denial of service(system crash) or possibly execute arbitrary code. **CVE ID : CVE-2019-14814**	N/A	O-LIN-LINU-141019/500
Buffer Copy without Checking Size of Input ('Classic Buffer	20-09-2019	7.2	There is heap-based buffer overflow in kernel, all versions up to, excluding 5.3, in the marvell wifi chip driver in Linux kernel, that allows local users to cause a	N/A	O-LIN-LINU-141019/501

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			denial of service(system crash) or possibly execute arbitrary code. **CVE ID : CVE-2019-14816**		
Out-of-bounds Write	19-09-2019	7.2	An out-of-bounds access issue was found in the Linux kernel, all versions through 5.3, in the way Linux kernel's KVM hypervisor implements the Coalesced MMIO write operation. It operates on an MMIO ring buffer 'struct kvm_coalesced_mmio' object, wherein write indices 'ring->first' and 'ring->last' value could be supplied by a host user-space process. An unprivileged host user or process with access to '/dev/kvm' device could use this flaw to crash the host kernel, resulting in a denial of service or potentially escalating privileges on the system. **CVE ID : CVE-2019-14821**	N/A	O-LIN-LINU-141019/502
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-09-2019	7.2	A buffer overflow flaw was found, in versions from 2.6.34 to 5.2.x, in the way Linux kernel's vhost functionality that translates virtqueue buffers to IOVs, logged the buffer descriptors during migration. A privileged guest user able to pass descriptors with invalid length to the host when migration is underway, could use this flaw to increase their privileges on	N/A	O-LIN-LINU-141019/503

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the host. **CVE ID : CVE-2019-14835**		
Loop with Unreachable Exit Condition ('Infinite Loop')	18-09-2019	5	An issue was discovered in the Linux kernel before 5.0.4. The 9p filesystem did not protect i_size_write() properly, which causes an i_size_read() infinite loop and denial of service on SMP systems. **CVE ID : CVE-2019-16413**	N/A	O-LIN-LINU-141019/504
Improper Initialization	27-09-2019	5	In the Linux kernel before 4.17, hns_roce_alloc_ucontext in drivers/infiniband/hw/hns/hns_roce_main.c does not initialize the resp data structure, which might allow attackers to obtain sensitive information from kernel stack memory, aka CID-df7e40425813. **CVE ID : CVE-2019-16921**	N/A	O-LIN-LINU-141019/505
mi					
xiaomi_millet_firmware					
Unrestricted Upload of File with Dangerous Type	18-09-2019	5.8	A malicious file upload vulnerability was discovered in Xiaomi Millet mobile phones 1-6.3.9.3. A particular condition involving a man-in-the-middle attack may lead to partial data leakage or malicious file writing. **CVE ID : CVE-2019-15843**	https://sec.xiaomi.com/post/152	O-MI-XIAO-141019/506
nxp					
kinetis_k8x_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	24-09-2019	4.6	On NXP Kinetis KV1x, Kinetis KV3x, and Kinetis K8x devices, Flash Access Controls (FAC) (a software IP protection method for execute-only access) can be defeated by leveraging a load instruction inside the execute-only region to expose the protected code into a CPU register. **CVE ID : CVE-2019-14239**	N/A	O-NXP-KINE-141019/507
kinetis_kv1x_firmware					
Improper Authentication	24-09-2019	4.6	On NXP Kinetis KV1x, Kinetis KV3x, and Kinetis K8x devices, Flash Access Controls (FAC) (a software IP protection method for execute-only access) can be defeated by leveraging a load instruction inside the execute-only region to expose the protected code into a CPU register. **CVE ID : CVE-2019-14239**	N/A	O-NXP-KINE-141019/508
kinetis_kv3x_firmware					
Improper Authentication	24-09-2019	4.6	On NXP Kinetis KV1x, Kinetis KV3x, and Kinetis K8x devices, Flash Access Controls (FAC) (a software IP protection method for execute-only access) can be defeated by leveraging a load instruction inside the execute-only region to expose the protected code into a CPU register. **CVE ID : CVE-2019-14239**	N/A	O-NXP-KINE-141019/509

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Opensuse					
leap					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	25-09-2019	6.8	It was discovered that there was a ECDSA timing attack in the libgcrypt20 cryptographic library. Version affected: 1.8.4-5, 1.7.6-2+deb9u3, and 1.6.3-2+deb8u4. Versions fixed: 1.8.5-2 and 1.6.3-2+deb8u7. **CVE ID : CVE-2019-13627**	N/A	O-OPE-LEAP-141019/510
Redhat					
virtualization					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-09-2019	7.2	A buffer overflow flaw was found, in versions from 2.6.34 to 5.2.x, in the way Linux kernel's vhost functionality that translates virtqueue buffers to IOVs, logged the buffer descriptors during migration. A privileged guest user able to pass descriptors with invalid length to the host when migration is underway, could use this flaw to increase their privileges on the host. **CVE ID : CVE-2019-14835**	N/A	O-RED-VIRT-141019/511
enterprise_linux					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-09-2019	7.2	There is heap-based buffer overflow in Linux kernel, all versions up to, excluding 5.3, in the marvell wifi chip driver in Linux kernel, that allows local users to cause a denial of service(system crash) or possibly execute	N/A	O-RED-ENTE-141019/512

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code. **CVE ID : CVE-2019-14814**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-09-2019	7.2	There is heap-based buffer overflow in kernel, all versions up to, excluding 5.3, in the marvell wifi chip driver in Linux kernel, that allows local users to cause a denial of service(system crash) or possibly execute arbitrary code. **CVE ID : CVE-2019-14816**	N/A	O-RED-ENTE-141019/513
Out-of-bounds Write	19-09-2019	7.2	An out-of-bounds access issue was found in the Linux kernel, all versions through 5.3, in the way Linux kernel's KVM hypervisor implements the Coalesced MMIO write operation. It operates on an MMIO ring buffer 'struct kvm_coalesced_mmio' object, wherein write indices 'ring->first' and 'ring->last' value could be supplied by a host user-space process. An unprivileged host user or process with access to '/dev/kvm' device could use this flaw to crash the host kernel, resulting in a denial of service or potentially escalating privileges on the system. **CVE ID : CVE-2019-14821**	N/A	O-RED-ENTE-141019/514
Insufficient Session Expiration	17-09-2019	2.1	A flaw was found in FreeIPA versions 4.5.0 and later. Session cookies were retained in the cache after logout. An attacker could	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-	O-RED-ENTE-141019/515

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			abuse this flaw if they obtain previously valid session cookies and can use this to gain access to the session. **CVE ID : CVE-2019-14826**	14826	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-09-2019	7.2	A buffer overflow flaw was found, in versions from 2.6.34 to 5.2.x, in the way Linux kernel's vhost functionality that translates virtqueue buffers to IOVs, logged the buffer descriptors during migration. A privileged guest user able to pass descriptors with invalid length to the host when migration is underway, could use this flaw to increase their privileges on the host. **CVE ID : CVE-2019-14835**	N/A	O-RED-ENTE-141019/516
messaging_realtime_grid					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-09-2019	7.2	There is heap-based buffer overflow in Linux kernel, all versions up to, excluding 5.3, in the marvell wifi chip driver in Linux kernel, that allows local users to cause a denial of service(system crash) or possibly execute arbitrary code. **CVE ID : CVE-2019-14814**	N/A	O-RED-MESS-141019/517
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-09-2019	7.2	There is heap-based buffer overflow in kernel, all versions up to, excluding 5.3, in the marvell wifi chip driver in Linux kernel, that allows local users to cause a denial of service(system	N/A	O-RED-MESS-141019/518

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crash) or possibly execute arbitrary code. **CVE ID : CVE-2019-14816**		
Schneider-electric					
modicon_premium_firmware					
Improper Handling of Exceptional Conditions	17-09-2019	7.8	A CWE-248: Uncaught Exception vulnerability exists in Modicon M580 (firmware versions prior to V2.90), Modicon M340 (firmware versions prior to V3.10), Modicon Premium (all versions), Modicon Quantum (all versions), which could cause a possible denial of service when reading invalid data from the controller. **CVE ID : CVE-2019-6809**	https://www.schneider-electric.com/en/download/document/SEVD-2019-134-11/	O-SCH-MODI-141019/519
Improper Handling of Exceptional Conditions	17-09-2019	7.8	A CWE-248: Uncaught Exception vulnerability exists Modicon M580 (firmware version prior to V2.90), Modicon M340 (firmware version prior to V3.10), Modicon Premium (all versions), and Modicon Quantum (all versions), which could cause a possible denial of service when reading specific coils and registers in the controller over Modbus. **CVE ID : CVE-2019-6828**	https://www.schneider-electric.com/en/download/document/SEVD-2019-134-11/	O-SCH-MODI-141019/520
modicon_quantum_firmware					
Improper Handling of Exceptional	17-09-2019	7.8	A CWE-248: Uncaught Exception vulnerability exists in Modicon M580	https://www.schneider-	O-SCH-MODI-141019/521

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Conditions			(firmware versions prior to V2.90), Modicon M340 (firmware versions prior to V3.10), Modicon Premium (all versions), Modicon Quantum (all versions), which could cause a possible denial of service when reading invalid data from the controller. **CVE ID : CVE-2019-6809**	electric.com/en/download/document/SEVD-2019-134-11/	
Improper Handling of Exceptional Conditions	17-09-2019	7.8	A CWE-248: Uncaught Exception vulnerability exists Modicon M580 (firmware version prior to V2.90), Modicon M340 (firmware version prior to V3.10), Modicon Premium (all versions), and Modicon Quantum (all versions), which could cause a possible denial of service when reading specific coils and registers in the controller over Modbus. **CVE ID : CVE-2019-6828**	https://www.schneider-electric.com/en/download/document/SEVD-2019-134-11/	O-SCH-MODI-141019/522
modicon_m340_firmware					
Improper Check for Unusual or Exceptional Conditions	17-09-2019	7.8	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in BMXNOR0200H Ethernet / Serial RTU module (all firmware versions) and Modicon M340 controller (all firmware versions), which could cause denial of service when truncated SNMP packets on port 161/UDP	https://www.schneider-electric.com/en/download/document/SEVD-2019-225-03/	O-SCH-MODI-141019/523

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			are received by the device. **CVE ID : CVE-2019-6813**		
modicon_quantum_140noe77101_firmware					
Improper Check for Unusual or Exceptional Conditions	17-09-2019	5	An Improper Check for Unusual or Exceptional Conditions (CWE-754) vulnerability exists in Modicon Quantum 140 NOE771x1 version 6.9 and earlier, which could cause denial of service when the module receives an IP fragmented packet with a length greater than 65535 bytes. The module then requires a power cycle to recover. **CVE ID : CVE-2019-6811**	https://www.schneider-electric.com/en/download/document/SEVD-2019-253-02/	O-SCH-MODI-141019/524
modicon_quantum_140noe77111_firmware					
Improper Check for Unusual or Exceptional Conditions	17-09-2019	5	An Improper Check for Unusual or Exceptional Conditions (CWE-754) vulnerability exists in Modicon Quantum 140 NOE771x1 version 6.9 and earlier, which could cause denial of service when the module receives an IP fragmented packet with a length greater than 65535 bytes. The module then requires a power cycle to recover. **CVE ID : CVE-2019-6811**	https://www.schneider-electric.com/en/download/document/SEVD-2019-253-02/	O-SCH-MODI-141019/525
hmigto_firmware					
Improper Check for Unusual or	17-09-2019	4.3	A CWE-754 ? Improper Check for Unusual or Exceptional Conditions	https://www.schneider-	O-SCH-HMIG-141019/526

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exceptional Conditions			vulnerability exists in Magelis HMI Panels (all versions of - HMIGTO, HMISTO, XBTGH, HMIGTU, HMIGTUX, HMISCU, HMISTU, XBTGT, XBTGT, HMIGXO, HMIGXU), which could cause a temporary freeze of the HMI when a high rate of frames is received. When the attack stops, the buffered commands are processed by the HMI panel. **CVE ID : CVE-2019-6833**	electric.com /ww/en/do wnload/doc ument/SEV D-2019-225-01	
hmigxo_firmware					
Improper Check for Unusual or Exceptional Conditions	17-09-2019	4.3	A CWE-754 ? Improper Check for Unusual or Exceptional Conditions vulnerability exists in Magelis HMI Panels (all versions of - HMIGTO, HMISTO, XBTGH, HMIGTU, HMIGTUX, HMISCU, HMISTU, XBTGT, XBTGT, HMIGXO, HMIGXU), which could cause a temporary freeze of the HMI when a high rate of frames is received. When the attack stops, the buffered commands are processed by the HMI panel. **CVE ID : CVE-2019-6833**	https://ww w.schneider - electric.com /ww/en/do wnload/doc ument/SEV D-2019-225-01	O-SCH-HMIG-141019/527
hmigxu_firmware					
Improper Check for Unusual or Exceptional Conditions	17-09-2019	4.3	A CWE-754 ? Improper Check for Unusual or Exceptional Conditions vulnerability exists in Magelis HMI Panels (all versions of - HMIGTO,	https://ww w.schneider - electric.com /ww/en/do wnload/doc	O-SCH-HMIG-141019/528

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			HMISTO, XBTGH, HMIGTU, HMIGTUX, HMISCU, HMISTU, XBTGT, XBTGT, HMIGXO, HMIGXU), which could cause a temporary freeze of the HMI when a high rate of frames is received. When the attack stops, the buffered commands are processed by the HMI panel. **CVE ID : CVE-2019-6833**	ument/SEVD-2019-225-01	
hmiscu_firmware					
Improper Check for Unusual or Exceptional Conditions	17-09-2019	4.3	A CWE-754 ? Improper Check for Unusual or Exceptional Conditions vulnerability exists in Magelis HMI Panels (all versions of - HMIGTO, HMISTO, XBTGH, HMIGTU, HMIGTUX, HMISCU, HMISTU, XBTGT, XBTGT, HMIGXO, HMIGXU), which could cause a temporary freeze of the HMI when a high rate of frames is received. When the attack stops, the buffered commands are processed by the HMI panel. **CVE ID : CVE-2019-6833**	https://www.schneider-electric.com/ww/en/download/document/SEVD-2019-225-01	O-SCH-HMIS-141019/529
hmisto_firmware					
Improper Check for Unusual or Exceptional Conditions	17-09-2019	4.3	A CWE-754 ? Improper Check for Unusual or Exceptional Conditions vulnerability exists in Magelis HMI Panels (all versions of - HMIGTO, HMISTO, XBTGH, HMIGTU, HMIGTUX, HMISCU, HMISTU, XBTGT, XBTGT, HMIGXO,	https://www.schneider-electric.com/ww/en/download/document/SEVD-2019-225-01	O-SCH-HMIS-141019/530

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			HMIGXU), which could cause a temporary freeze of the HMI when a high rate of frames is received. When the attack stops, the buffered commands are processed by the HMI panel. **CVE ID : CVE-2019-6833**		
hmistu_firmware					
Improper Check for Unusual or Exceptional Conditions	17-09-2019	4.3	A CWE-754 ? Improper Check for Unusual or Exceptional Conditions vulnerability exists in Magelis HMI Panels (all versions of - HMIGTO, HMISTO, XBTGH, HMIGTU, HMIGTUX, HMISCU, HMISTU, XBTGT, XBTGT, HMIGXO, HMIGXU), which could cause a temporary freeze of the HMI when a high rate of frames is received. When the attack stops, the buffered commands are processed by the HMI panel. **CVE ID : CVE-2019-6833**	https://www.schneider-electric.com/ww/en/download/document/SEVD-2019-225-01	O-SCH-HMIS-141019/531
xbtgh_firmware					
Improper Check for Unusual or Exceptional Conditions	17-09-2019	4.3	A CWE-754 ? Improper Check for Unusual or Exceptional Conditions vulnerability exists in Magelis HMI Panels (all versions of - HMIGTO, HMISTO, XBTGH, HMIGTU, HMIGTUX, HMISCU, HMISTU, XBTGT, XBTGT, HMIGXO, HMIGXU), which could cause a temporary freeze of the HMI when a high rate of	https://www.schneider-electric.com/ww/en/download/document/SEVD-2019-225-01	O-SCH-XBTG-141019/532

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			frames is received. When the attack stops, the buffered commands are processed by the HMI panel. **CVE ID : CVE-2019-6833**		
xbtgt_firmware					
Improper Check for Unusual or Exceptional Conditions	17-09-2019	4.3	A CWE-754 ? Improper Check for Unusual or Exceptional Conditions vulnerability exists in Magelis HMI Panels (all versions of - HMIGTO, HMISTO, XBTGH, HMIGTU, HMIGTUX, HMISCU, HMISTU, XBTGT, XBTGT, HMIGXO, HMIGXU), which could cause a temporary freeze of the HMI when a high rate of frames is received. When the attack stops, the buffered commands are processed by the HMI panel. **CVE ID : CVE-2019-6833**	https://www.schneider-electric.com/ww/en/download/document/SEVD-2019-225-01	O-SCH-XBTG-141019/533
bmxnor0200h_firmware					
Incorrect Authorization	17-09-2019	6.5	CWE-284: Improper Access Control vulnerability exists in BMXNOR0200H Ethernet / Serial RTU module (all firmware versions), which could cause the execution of commands by unauthorized users when using IEC 60870-5-104 protocol. **CVE ID : CVE-2019-6810**	https://www.schneider-electric.com/en/download/document/SEVD-2019-225-03/	O-SCH-BMXN-141019/534
Improper Check for Unusual or Exceptional	17-09-2019	7.8	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in BMXNOR0200H Ethernet / Serial RTU	https://www.schneider-electric.com/en/downlo	O-SCH-BMXN-141019/535

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Conditions			module (all firmware versions) and Modicon M340 controller (all firmware versions), which could cause denial of service when truncated SNMP packets on port 161/UDP are received by the device. **CVE ID : CVE-2019-6813**	ad/document/SEVD-2019-225-03/	
Improper Check for Unusual or Exceptional Conditions	17-09-2019	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in BMXNOR0200H Ethernet / Serial RTU module (all firmware versions), which could cause disconnection of active connections when an unusually high number of IEC 60870- 5-104 packets are received by the module on port 2404/TCP. **CVE ID : CVE-2019-6831**	https://www.schneider-electric.com/en/download/document/SEVD-2019-225-03/	O-SCH-BMXN-141019/536
sick					
fx0-gent00000_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	24-09-2019	5	SICK FX0-GPNT00000 and FX0-GENT00000 devices through 3.4.0 have a Buffer Overflow **CVE ID : CVE-2019-14753**	https://www.sick.com/medias/SCA-2019-002.pdf?context=bWFzdGVyfGNvbnRlbnR8MjE5MDk1fGFwcGxpY2F0aW9uL3BkZnxjb250ZW50L2g3Yy9oNDEvMT	O-SIC-FX0--141019/537

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				AzMDY0NjAzNTI1NDIucGRmfDJlZTVmZjJmYzYwYmQ1ODQyZDBmMjA0OTc3ZDBjMmY1YzZkYzUzNzI0MWI0OGIyOTE0OTllY2VlYjJhNzUzYTE	
fx0-gpnt00000_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	24-09-2019	5	SICK FX0-GPNT00000 and FX0-GENT00000 devices through 3.4.0 have a Buffer Overflow **CVE ID : CVE-2019-14753**	https://www.sick.com/medias/SCA-2019-002.pdf?context=bWFzdGVyfGNvbnRlbnR8MjE5MDk1fGFwcGxpY2F0aW9uL3BkZnxjb250ZW50L2g3Yy9oNDEvMTAzMDY0NjAzNTI1NDIucGRmfDJlZTVmZjJmYzYwYmQ1ODQyZDBmMjA0OTc3ZDBjMmY1YzZkYzUzNzI0MWI0OGIyOTE0OTllY2VlYjJhNzUzYT	O-SIC-FX0--141019/538

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				E	
ST					
stm32f4_firmware					
Improper Authenticati on	24-09-2019	4.6	On STMicroelectronics STM32F7 devices, Proprietary Code Read Out Protection (PCROP) (a software IP protection method) can be defeated with a debug probe via the Instruction Tightly Coupled Memory (ITCM) bus. **CVE ID : CVE-2019-14238**	N/A	O-ST-STM3-141019/539
stm32f7_firmware					
Improper Authenticati on	24-09-2019	4.6	On STMicroelectronics STM32F7 devices, Proprietary Code Read Out Protection (PCROP) (a software IP protection method) can be defeated with a debug probe via the Instruction Tightly Coupled Memory (ITCM) bus. **CVE ID : CVE-2019-14238**	N/A	O-ST-STM3-141019/540
stm32h7_firmware					
Improper Authenticati on	24-09-2019	4.6	On STMicroelectronics STM32F7 devices, Proprietary Code Read Out Protection (PCROP) (a software IP protection method) can be defeated with a debug probe via the Instruction Tightly Coupled Memory (ITCM) bus. **CVE ID : CVE-2019-14238**	N/A	O-ST-STM3-141019/541
stm32l0_firmware					
Improper	24-09-2019	4.6	On STMicroelectronics	N/A	O-ST-STM3-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Authentication			STM32F7 devices, Proprietary Code Read Out Protection (PCROP) (a software IP protection method) can be defeated with a debug probe via the Instruction Tightly Coupled Memory (ITCM) bus. **CVE ID : CVE-2019-14238**		141019/542
stm32l1_firmware					
Improper Authentication	24-09-2019	4.6	On STMicroelectronics STM32F7 devices, Proprietary Code Read Out Protection (PCROP) (a software IP protection method) can be defeated with a debug probe via the Instruction Tightly Coupled Memory (ITCM) bus. **CVE ID : CVE-2019-14238**	N/A	O-ST-STM3-141019/543
stm32l4_firmware					
Improper Authentication	24-09-2019	4.6	On STMicroelectronics STM32F7 devices, Proprietary Code Read Out Protection (PCROP) (a software IP protection method) can be defeated with a debug probe via the Instruction Tightly Coupled Memory (ITCM) bus. **CVE ID : CVE-2019-14238**	N/A	O-ST-STM3-141019/544
Supermicro					
x10drt-ps_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in	N/A	O-SUP-X10D-141019/545

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10D-141019/546
x10drt-pt_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-X10D-141019/547

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-16649		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10D-141019/548
x10drt-p_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10D-141019/549
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker	N/A	O-SUP-X10D-141019/550

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		
x10drt-pibf_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10D-141019/551
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10D-141019/552
x10drt-pibq_firmware					
Use of Hard-coded	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11	N/A	O-SUP-X10D-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Credentials			products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		141019/553
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10D-141019/554
x10drw-i_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices	N/A	O-SUP-X10D-141019/555

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10D-141019/556
x10dsc+_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10D-141019/557
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor	N/A	O-SUP-X10D-141019/558

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		
x10qbl-ct_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10Q-141019/559
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10Q-141019/560
x10qbl_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10Q-141019/561
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10Q-141019/562
x10qrh+_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can	N/A	O-SUP-X10Q-141019/563

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10Q-141019/564
x10sae_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10S-141019/565
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different	N/A	O-SUP-X10S-141019/566

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		
x10sat_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10S-141019/567
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-X10S-141019/568

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-16650		
x10sdd-16c-f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10S-141019/569
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10S-141019/570
x10sdd-f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC	N/A	O-SUP-X10S-141019/571

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10S-141019/572
x10sde-df_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10S-141019/573
Improper	20-09-2019	7.5	On Supermicro X10 and X11	N/A	O-SUP-X10S-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		141019/574
x10sdv-12c+-tln4f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10S-141019/575
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB	N/A	O-SUP-X10S-141019/576

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		
x10sdv-12c-tln4f+_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10S-141019/577
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10S-141019/578
x10sdv-12c-tln4f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in	N/A	O-SUP-X10S-141019/579

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10S-141019/580
x10sdv-16c+-tln4f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-X10S-141019/581

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-16649		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10S-141019/582
x10sdv-16c-tln4f+_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10S-141019/583
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker	N/A	O-SUP-X10S-141019/584

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		
x10sdv-16c-tln4f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10S-141019/585
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10S-141019/586
x10sdv-2c-7tp4f_firmware					
Use of Hard-coded	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11	N/A	O-SUP-X10S-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Credentials			products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		141019/587
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10S-141019/588
x10sdv-2c-tln2f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices	N/A	O-SUP-X10S-141019/589

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10S-141019/590
x10sdv-2c-tp4f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10S-141019/591
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor	N/A	O-SUP-X10S-141019/592

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		
x10sdv-2c-tp8f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10S-141019/593
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10S-141019/594
x10sdv-4c+-tln4f_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10S-141019/595
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10S-141019/596
x10sdv-4c+-tp4f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can	N/A	O-SUP-X10S-141019/597

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10S-141019/598
x10sdv-4c-7tp4f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10S-141019/599
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different	N/A	O-SUP-X10S-141019/600

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		
x10sdv-4c-tln2f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10S-141019/601
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-X10S-141019/602

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-16650		
x10sdv-4c-tln4f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10S-141019/603
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10S-141019/604
x10sdv-6c+-tln4f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC	N/A	O-SUP-X10S-141019/605

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10S-141019/606
x10sdv-6c-tln4f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10S-141019/607
Improper	20-09-2019	7.5	On Supermicro X10 and X11	N/A	O-SUP-X10S-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		141019/608
x10sdv-7tp4f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10S-141019/609
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB	N/A	O-SUP-X10S-141019/610

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		
x10sdv-7tp8f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10S-141019/611
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10S-141019/612
x10sdv-8c+-ln2f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in	N/A	O-SUP-X10S-141019/613

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10S-141019/614
x10sdv-8c-tln4f+_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-X10S-141019/615

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-16649		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10S-141019/616
x10sdv-8c-tln4f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10S-141019/617
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker	N/A	O-SUP-X10S-141019/618

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		
x10sdv-f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10S-141019/619
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10S-141019/620
x10sdv-tln4f_firmware					
Use of Hard-coded	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11	N/A	O-SUP-X10S-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Credentials			products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		141019/621
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10S-141019/622
x10sdv-tp8f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices	N/A	O-SUP-X10S-141019/623

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10S-141019/624
x10sl7-f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10S-141019/625
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor	N/A	O-SUP-X10S-141019/626

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		
x10sla-f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10S-141019/627
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10S-141019/628
x10sld-f_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10S-141019/629
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10S-141019/630
x10sld-hf_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can	N/A	O-SUP-X10S-141019/631

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10S-141019/632
x10sle-df_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10S-141019/633
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different	N/A	O-SUP-X10S-141019/634

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		
x10sle-f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10S-141019/635
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-X10S-141019/636

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-16650		
x10sle-hf_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10S-141019/637
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10S-141019/638
x10slh-f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC	N/A	O-SUP-X10S-141019/639

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10S-141019/640
x10sll+-f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10S-141019/641
Improper	20-09-2019	7.5	On Supermicro X10 and X11	N/A	O-SUP-X10S-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		141019/642
x10sll-f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10S-141019/643
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB	N/A	O-SUP-X10S-141019/644

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		
x10sll-s_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10S-141019/645
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10S-141019/646
x10sll-sf_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in	N/A	O-SUP-X10S-141019/647

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10S-141019/648
x10slm+-f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-X10S-141019/649

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-16649		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10S-141019/650
x10slm+-ln4f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10S-141019/651
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker	N/A	O-SUP-X10S-141019/652

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		
x10slm-f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10S-141019/653
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10S-141019/654
x10slx-f_firmware					
Use of Hard-coded	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11	N/A	O-SUP-X10S-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Credentials			products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		141019/655
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10S-141019/656
x10sra-f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices	N/A	O-SUP-X10S-141019/657

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10S-141019/658
x10sra_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10S-141019/659
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor	N/A	O-SUP-X10S-141019/660

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		
x10srd-f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10S-141019/661
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10S-141019/662
x10srg-f_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10S-141019/663
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10S-141019/664
x10srh-cf_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can	N/A	O-SUP-X10S-141019/665

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10S-141019/666
x10srh-cln4f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10S-141019/667
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different	N/A	O-SUP-X10S-141019/668

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		
x10sri-f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10S-141019/669
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-X10S-141019/670

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-16650		
x10srl-f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10S-141019/671
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10S-141019/672
x10srm-f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC	N/A	O-SUP-X10S-141019/673

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10S-141019/674
x10srm-tf_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10S-141019/675
Improper	20-09-2019	7.5	On Supermicro X10 and X11	N/A	O-SUP-X10S-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		141019/676
x10srw-f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10S-141019/677
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB	N/A	O-SUP-X10S-141019/678

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		
x11dac_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X11D-141019/679
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X11D-141019/680
x11dai-n_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in	N/A	O-SUP-X11D-141019/681

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X11D-141019/682
x11ddw-l_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-X11D-141019/683

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-16649		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X11D-141019/684
x11ddw-nt_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X11D-141019/685
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker	N/A	O-SUP-X11D-141019/686

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		
x11dgo-t_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X11D-141019/687
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X11D-141019/688
x11dgq_firmware					
Use of Hard-coded	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11	N/A	O-SUP-X11D-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Credentials			products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		141019/689
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X11D-141019/690
x11dpff-sn_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices	N/A	O-SUP-X11D-141019/691

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X11D-141019/692
x11dpfr-s_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X11D-141019/693
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor	N/A	O-SUP-X11D-141019/694

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		
x11dpfr-sn_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X11D-141019/695
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X11D-141019/696
x11dpg-ot-cpu_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X11D-141019/697
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X11D-141019/698
x11dpg-qt_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can	N/A	O-SUP-X11D-141019/699

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X11D-141019/700
x11dpg-sn_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X11D-141019/701
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different	N/A	O-SUP-X11D-141019/702

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		
x11dph-i_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X11D-141019/703
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-X11D-141019/704

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-16650		
x11dph-t_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X11D-141019/705
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X11D-141019/706
x11dph-tq_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC	N/A	O-SUP-X11D-141019/707

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X11D-141019/708
x11dpi-n_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X11D-141019/709
Improper	20-09-2019	7.5	On Supermicro X10 and X11	N/A	O-SUP-X11D-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		141019/710
x11dpi-nt_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X11D-141019/711
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB	N/A	O-SUP-X11D-141019/712

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		
x11dpl-i_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X11D-141019/713
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X11D-141019/714
x11dps-re_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in	N/A	O-SUP-X11D-141019/715

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X11D-141019/716
x11dpt-b_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-X11D-141019/717

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-16649		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X11D-141019/718
x11dpt-bh_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X11D-141019/719
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker	N/A	O-SUP-X11D-141019/720

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		
x11dpt-l_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X11D-141019/721
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X11D-141019/722
x11dpt-ps_firmware					
Use of Hard-coded	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11	N/A	O-SUP-X11D-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Credentials			products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		141019/723
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X11D-141019/724
x11dpu-v_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices	N/A	O-SUP-X11D-141019/725

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X11D-141019/726
x11dpu-x_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X11D-141019/727
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor	N/A	O-SUP-X11D-141019/728

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		
x11dpu-xll_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X11D-141019/729
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X11D-141019/730
x11dpu-z+_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X11D-141019/731
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X11D-141019/732
x11dpu-ze+_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can	N/A	O-SUP-X11D-141019/733

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X11D-141019/734
x11dpu_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X11D-141019/735
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different	N/A	O-SUP-X11D-141019/736

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		
x11dpx-t_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X11D-141019/737
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-X11D-141019/738

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-16650		
x11dsc+_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X11D-141019/739
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X11D-141019/740
x11dsf-e_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC	N/A	O-SUP-X11D-141019/741

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X11D-141019/742
x11dsn-ts_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X11D-141019/743
Improper	20-09-2019	7.5	On Supermicro X10 and X11	N/A	O-SUP-X11D-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		141019/744
x11dsn-tsq_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X11D-141019/745
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB	N/A	O-SUP-X11D-141019/746

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		
x11opi-cpu_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X11O-141019/747
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X11O-141019/748
x11qph+_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in	N/A	O-SUP-X11Q-141019/749

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X11Q-141019/750
x11sca-f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-X11S-141019/751

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-16649		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X11S-141019/752
x11sca-w_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X11S-141019/753
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker	N/A	O-SUP-X11S-141019/754

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		
x11sca_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X11S-141019/755
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X11S-141019/756
x11scd-f_firmware					
Use of Hard-coded	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11	N/A	O-SUP-X11S-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Credentials			products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		141019/757
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X11S-141019/758
x11sch-f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices	N/A	O-SUP-X11S-141019/759

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X11S-141019/760
x11sch-ln4f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X11S-141019/761
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor	N/A	O-SUP-X11S-141019/762

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		
x11scl-f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X11S-141019/763
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X11S-141019/764
x11scl-if_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X11S-141019/765
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X11S-141019/766
x11scl-ln4f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can	N/A	O-SUP-X11S-141019/767

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X11S-141019/768
x11scm-f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X11S-141019/769
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different	N/A	O-SUP-X11S-141019/770

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		
x11scm-ln8f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X11S-141019/771
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-X11S-141019/772

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-16650		
x11scw-f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X11S-141019/773
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X11S-141019/774
x11sdd-18c-f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC	N/A	O-SUP-X11S-141019/775

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X11S-141019/776
x11sdd-8c-f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X11S-141019/777
Improper	20-09-2019	7.5	On Supermicro X10 and X11	N/A	O-SUP-X11S-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		141019/778
x11sds-12c_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X11S-141019/779
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB	N/A	O-SUP-X11S-141019/780

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		
x11sds-16c_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X11S-141019/781
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X11S-141019/782
x11sds-8c_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in	N/A	O-SUP-X11S-141019/783

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X11S-141019/784
x11spa-t_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-X11S-141019/785

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-16649		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X11S-141019/786
x11spa-tf_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X11S-141019/787
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker	N/A	O-SUP-X11S-141019/788

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		
x11spg-tf_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X11S-141019/789
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X11S-141019/790
x11sph-nctf_firmware					
Use of Hard-coded	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11	N/A	O-SUP-X11S-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Credentials			products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		141019/791
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X11S-141019/792
x11sph-nctpf_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices	N/A	O-SUP-X11S-141019/793

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X11S-141019/794
x11spi-tf_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X11S-141019/795
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor	N/A	O-SUP-X11S-141019/796

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		
x11spl-f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X11S-141019/797
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X11S-141019/798
x11spm-f_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X11S-141019/799
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X11S-141019/800
x11spm-tf_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can	N/A	O-SUP-X11S-141019/801

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X11S-141019/802
x11spm-tpf_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X11S-141019/803
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different	N/A	O-SUP-X11S-141019/804

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		
x11spw-ctf_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X11S-141019/805
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-X11S-141019/806

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-16650		
x11spw-tf_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X11S-141019/807
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X11S-141019/808
x11sri-if_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC	N/A	O-SUP-X11S-141019/809

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X11S-141019/810
x11srl-f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X11S-141019/811
Improper	20-09-2019	7.5	On Supermicro X10 and X11	N/A	O-SUP-X11S-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		141019/812
x11srm-f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X11S-141019/813
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB	N/A	O-SUP-X11S-141019/814

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		
x11srm-vf_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X11S-141019/815
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X11S-141019/816
x11ssd-f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in	N/A	O-SUP-X11S-141019/817

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X11S-141019/818
x11sse-f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-X11S-141019/819

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-16649		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X11S-141019/820
x11ssh-ctf_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X11S-141019/821
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker	N/A	O-SUP-X11S-141019/822

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		
x11ssh-f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X11S-141019/823
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X11S-141019/824
x11ssh-gf-1585_firmware					
Use of Hard-coded	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11	N/A	O-SUP-X11S-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Credentials			products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		141019/825
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X11S-141019/826
x11ssh-gf-1585l_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices	N/A	O-SUP-X11S-141019/827

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X11S-141019/828
x11ssh-gtf-1585_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X11S-141019/829
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor	N/A	O-SUP-X11S-141019/830

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		
x11ssh-gtf-1585l_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X11S-141019/831
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X11S-141019/832
x11ssh-ln4f_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X11S-141019/833
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X11S-141019/834
x11ssh-tf_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can	N/A	O-SUP-X11S-141019/835

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X11S-141019/836
x11ssi-ln4f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X11S-141019/837
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different	N/A	O-SUP-X11S-141019/838

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		
x11ssl-cf_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X11S-141019/839
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-X11S-141019/840

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-16650		
x11ssl-f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X11S-141019/841
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X11S-141019/842
x11ssl-nf_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC	N/A	O-SUP-X11S-141019/843

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X11S-141019/844
x11ssl_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X11S-141019/845
Improper	20-09-2019	7.5	On Supermicro X10 and X11	N/A	O-SUP-X11S-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		141019/846
x11ssm-f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X11S-141019/847
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB	N/A	O-SUP-X11S-141019/848

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		
x11ssm_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X11S-141019/849
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X11S-141019/850
x11ssw-4tf_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in	N/A	O-SUP-X11S-141019/851

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X11S-141019/852
x11ssw-f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-X11S-141019/853

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-16649		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X11S-141019/854
x11ssw-tf_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X11S-141019/855
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker	N/A	O-SUP-X11S-141019/856

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		
x9da7/e_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X9DA-141019/857
x9dai_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X9DA-141019/858

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
x9dal-3/i_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X9DA-141019/859
x9dax-7/i(t)f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X9DA-141019/860
x9dax-7/if-hft_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service	N/A	O-SUP-X9DA-141019/861

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
x9db3/i-(tp)f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X9DB-141019/862
x9dbl-3/i(f)_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the	N/A	O-SUP-X9DB-141019/863

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			BMC. **CVE ID : CVE-2019-16649**		
x9dbs-f(-2u)_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X9DB-141019/864
x9dbu-3/if_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X9DB-141019/865
x9dr/i-f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of	N/A	O-SUP-X9DR-141019/866

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
x9dr3/i-ln4f+_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X9DR-141019/867
x9dr7-jln4f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can	N/A	O-SUP-X9DR-141019/868

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
x9dr7/e-ln4f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X9DR-141019/869
x9dr7/e-tf+_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X9DR-141019/870
x9drd-7ln4f_series_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X9DR-141019/871
x9drd-c(n)t+_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X9DR-141019/872
x10dru-i+_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC	N/A	O-SUP-X10D-141019/873

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10D-141019/874
x10dru-x_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10D-141019/875
Improper	20-09-2019	7.5	On Supermicro X10 and X11	N/A	O-SUP-X10D-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		141019/876
x10dru-xll_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10D-141019/877
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB	N/A	O-SUP-X10D-141019/878

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		
x10drw-it_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10D-141019/879
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10D-141019/880
x10drw-nt_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in	N/A	O-SUP-X10D-141019/881

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10D-141019/882
x10qbl-4_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-X10Q-141019/883

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-16649		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10Q-141019/884
x10qbl-4ct_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10Q-141019/885
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker	N/A	O-SUP-X10Q-141019/886

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		
a1sa2-2750f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-A1SA-141019/887
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-A1SA-141019/888
a1sai-2550f_firmware					
Use of Hard-coded	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11	N/A	O-SUP-A1SA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Credentials			products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		141019/889
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-A1SA-141019/890
a1sai-2750f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices	N/A	O-SUP-A1SA-141019/891

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-A1SA-141019/892
a1sam-2550f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-A1SA-141019/893
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor	N/A	O-SUP-A1SA-141019/894

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		
a1sam-2750f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-A1SA-141019/895
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-A1SA-141019/896
a1sri-2358f_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-A1SR-141019/897
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-A1SR-141019/898
a1sri-2558f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can	N/A	O-SUP-A1SR-141019/899

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-A1SR-141019/900
a1sri-2758f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-A1SR-141019/901
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different	N/A	O-SUP-A1SR-141019/902

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		
a1srm-2558f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-A1SR-141019/903
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-A1SR-141019/904

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-16650		
a1srm-2758f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-A1SR-141019/905
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-A1SR-141019/906
a1srm-ln5f-2358_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC	N/A	O-SUP-A1SR-141019/907

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-A1SR-141019/908
a1srm-ln7f-2358_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-A1SR-141019/909
Improper	20-09-2019	7.5	On Supermicro X10 and X11	N/A	O-SUP-A1SR-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		141019/910
a1srm-ln7f-2758_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-A1SR-141019/911
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB	N/A	O-SUP-A1SR-141019/912

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		
b10drc-n_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-B10D-141019/913
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-B10D-141019/914
b10drc_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in	N/A	O-SUP-B10D-141019/915

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-B10D-141019/916
x10drff-ctg_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-X10D-141019/917

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-16649		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10D-141019/918
x10drff-ig_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10D-141019/919
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker	N/A	O-SUP-X10D-141019/920

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		
x10drff-itg_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10D-141019/921
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10D-141019/922
x10drff_firmware					
Use of Hard-coded	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11	N/A	O-SUP-X10D-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Credentials			products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		141019/923
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10D-141019/924
x10drfr-n_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices	N/A	O-SUP-X10D-141019/925

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10D-141019/926
x10drfr-nt_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10D-141019/927
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor	N/A	O-SUP-X10D-141019/928

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		
x10drfr-t_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10D-141019/929
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10D-141019/930
x10drfr_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10D-141019/931
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10D-141019/932
x10drg-h_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can	N/A	O-SUP-X10D-141019/933

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10D-141019/934
x10drg-ht_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10D-141019/935
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different	N/A	O-SUP-X10D-141019/936

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		
x10drg-o+-cpu_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10D-141019/937
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-X10D-141019/938

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-16650		
x10drg-ot+-cpu_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10D-141019/939
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10D-141019/940
x10drg-q_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC	N/A	O-SUP-X10D-141019/941

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10D-141019/942
x10drh-c_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10D-141019/943
Improper	20-09-2019	7.5	On Supermicro X10 and X11	N/A	O-SUP-X10D-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		141019/944
x10drh-cln4_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10D-141019/945
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB	N/A	O-SUP-X10D-141019/946

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		
x10drh-ct_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10D-141019/947
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10D-141019/948
x10drh-i_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in	N/A	O-SUP-X10D-141019/949

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10D-141019/950
x10drh-iln4_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-X10D-141019/951

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-16649		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10D-141019/952
x10drh-it_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10D-141019/953
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker	N/A	O-SUP-X10D-141019/954

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		
x10dri-ln4+_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10D-141019/955
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10D-141019/956
x10dri-t4+_firmware					
Use of Hard-coded	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11	N/A	O-SUP-X10D-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Credentials			products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		141019/957
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10D-141019/958
x10dri-t_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices	N/A	O-SUP-X10D-141019/959

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10D-141019/960
x10dri_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10D-141019/961
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor	N/A	O-SUP-X10D-141019/962

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		
x10drl-c_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10D-141019/963
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10D-141019/964
x10drl-ct_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10D-141019/965
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10D-141019/966
x10drl-i_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can	N/A	O-SUP-X10D-141019/967

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10D-141019/968
x10drl-it_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10D-141019/969
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different	N/A	O-SUP-X10D-141019/970

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		
x10drl-ln4_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10D-141019/971
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-X10D-141019/972

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-16650		
x10drs_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10D-141019/973
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10D-141019/974
x10drt-b+_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC	N/A	O-SUP-X10D-141019/975

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10D-141019/976
x10drt-h_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10D-141019/977
Improper	20-09-2019	7.5	On Supermicro X10 and X11	N/A	O-SUP-X10D-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		141019/978
x10drt-hibf_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10D-141019/979
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB	N/A	O-SUP-X10D-141019/980

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		
x10drt-l_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10D-141019/981
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10D-141019/982
x10drt-libf_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in	N/A	O-SUP-X10D-141019/983

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10D-141019/984
x10drt-libq_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-X10D-141019/985

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-16649		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10D-141019/986
x10drw-e_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10D-141019/987
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker	N/A	O-SUP-X10D-141019/988

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		
x10drw-et_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10D-141019/989
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10D-141019/990
x10drw-n_firmware					
Use of Hard-coded	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11	N/A	O-SUP-X10D-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Credentials			products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		141019/991
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10D-141019/992
x10drx_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices	N/A	O-SUP-X10D-141019/993

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10D-141019/994
x10dsn-ts_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10D-141019/995
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor	N/A	O-SUP-X10D-141019/996

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		
x10obi-cpu_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10O-141019/997
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10O-141019/998
x10qbi_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10Q-141019/999
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10Q-141019/1000
x9drd-ef_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can	N/A	O-SUP-X9DR-141019/1001

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
x9drd-it+_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X9DR-141019/1002
x9drd-l/if_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X9DR-141019/1003
x9drff(-7)_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X9DR-141019/1004
x9drff-7/i(t)+_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X9DR-141019/1005
x9drff-7/i(t)g+_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC	N/A	O-SUP-X9DR-141019/1006

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
x9drfr_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X9DR-141019/1007
x9drg-h(t)f+_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-X9DR-141019/1008

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-16649		
x9drg-h(t)f+ii_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X9DR-141019/1009
x9drg-h(t)f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X9DR-141019/1010
x9drg-o(t)f-cpu_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in	N/A	O-SUP-X9DR-141019/1011

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
x9drg-qf_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X9DR-141019/1012
x9drh-7/i(t)f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices	N/A	O-SUP-X9DR-141019/1013

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
x9drh-if-nv_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X9DR-141019/1014
x9drl-3/if_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X9DR-141019/1015
x9drl-7/ef_firmware					
Use of Hard-coded	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11	N/A	O-SUP-X9DR-141019/1016

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Credentials			products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
x9drt-h_series_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X9DR-141019/1017
x9drt-hf+_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual	N/A	O-SUP-X9DR-141019/1018

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
x9drt-p_series_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X9DR-141019/1019
x9drt_series_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X9DR-141019/1020

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
x9drw-3/if_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X9DR-141019/1021
x9drw-3ln4f+/3tf+_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X9DR-141019/1022
x9drw-7/itpf+_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service	N/A	O-SUP-X9DR-141019/1023

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
x9drw-7/itpf_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X9DR-141019/1024
x9drw-c(t)f31_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the	N/A	O-SUP-X9DR-141019/1025

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			BMC. **CVE ID : CVE-2019-16649**		
x9drx+-f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X9DR-141019/1026
x9qr7-tf+_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X9QR-141019/1027
x9qr7-tf_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of	N/A	O-SUP-X9QR-141019/1028

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
x9qri-f+_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X9QR-141019/1029
x9qri-f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can	N/A	O-SUP-X9QR-141019/1030

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
x9sae(-v)_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X9SA-141019/1031
x9sca(-f)_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X9SC-141019/1032
x9scd_series_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X9SC-141019/1033
x9sci-ln4(f)_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X9SC-141019/1034
x9scl(-f)_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC	N/A	O-SUP-X9SC-141019/1035

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
x9scl+-f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X9SC-141019/1036
x9scm(-f)_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-X9SC-141019/1037

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-16649		
x9sra_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X9SR-141019/1038
x9srd-f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X9SR-141019/1039
x9sre/i_series_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in	N/A	O-SUP-X9SR-141019/1040

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
x9srg-f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X9SR-141019/1041
x9srh-7(t)f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices	N/A	O-SUP-X9SR-141019/1042

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
x9srl(-f)_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X9SR-141019/1043
x9srw-f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X9SR-141019/1044
b10drg-ibf2_firmware					
Use of Hard-coded	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11	N/A	O-SUP-B10D-141019/1045

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Credentials			products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-B10D-141019/1046
b10drg-ibf_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices	N/A	O-SUP-B10D-141019/1047

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-B10D-141019/1048
b10drg-tp_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-B10D-141019/1049
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor	N/A	O-SUP-B10D-141019/1050

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		
b10dri-n_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-B10D-141019/1051
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-B10D-141019/1052
b10dri_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-B10D-141019/1053
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-B10D-141019/1054
b10drt-ibf2_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can	N/A	O-SUP-B10D-141019/1055

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-B10D-141019/1056
b10drt-ibf_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-B10D-141019/1057
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different	N/A	O-SUP-B10D-141019/1058

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		
b10drt-tp_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-B10D-141019/1059
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-B10D-141019/1060

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-16650		
b10drt_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-B10D-141019/1061
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-B10D-141019/1062
b11dpe_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC	N/A	O-SUP-B11D-141019/1063

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-B11D-141019/1064
b11dpt_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-B11D-141019/1065
Improper	20-09-2019	7.5	On Supermicro X10 and X11	N/A	O-SUP-B11D-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		141019/1066
b11qpi_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-B11Q-141019/1067
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB	N/A	O-SUP-B11Q-141019/1068

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		
b11spe-cpu-25g_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-B11S-141019/1069
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-B11S-141019/1070
b11spe-cpu-tf_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in	N/A	O-SUP-B11S-141019/1071

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-B11S-141019/1072
b1sd1-16c-tf_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-B1SD-141019/1073

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-16649		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-B1SD-141019/1074
b1sd1-tf_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-B1SD-141019/1075
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker	N/A	O-SUP-B1SD-141019/1076

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		
b1sd2-16c-tf_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-B1SD-141019/1077
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-B1SD-141019/1078
b1sd2-tf_firmware					
Use of Hard-coded	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11	N/A	O-SUP-B1SD-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Credentials			products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		141019/1079
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-B1SD-141019/1080
b2ss1-cf_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices	N/A	O-SUP-B2SS-141019/1081

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-B2SS-141019/1082
b2ss1-cpu_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-B2SS-141019/1083
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor	N/A	O-SUP-B2SS-141019/1084

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		
b2ss1-f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-B2SS-141019/1085
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-B2SS-141019/1086
b2ss1-h-mtf_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-B2SS-141019/1087
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-B2SS-141019/1088
b2ss1-mtf_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can	N/A	O-SUP-B2SS-141019/1089

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-B2SS-141019/1090
b2ss2-f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-B2SS-141019/1091
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different	N/A	O-SUP-B2SS-141019/1092

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		
b2ss2-h-mtf_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-B2SS-141019/1093
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-B2SS-141019/1094

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-16650		
b2ss2-mtf_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-B2SS-141019/1095
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-B2SS-141019/1096
b9dr7_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC	N/A	O-SUP-B9DR-141019/1097

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
b9drg-3m_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-B9DR-141019/1098
b9drg-e_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-B9DR-141019/1099

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-16649		
b9drg_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-B9DR-141019/1100
b9dri_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-B9DR-141019/1101
b9drp_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in	N/A	O-SUP-B9DR-141019/1102

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
b9drt_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-B9DR-141019/1103
b9qr7(-tp)_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices	N/A	O-SUP-B9QR-141019/1104

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
m11sdv-4c-ln4f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-M11S-141019/1105
m11sdv-4ct-ln4f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-M11S-141019/1106
m11sdv-8c+-ln4f_firmware					
Use of Hard-coded	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11	N/A	O-SUP-M11S-141019/1107

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Credentials			products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
m11sdv-8c-ln4f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-M11S-141019/1108
m11sdv-8ct-ln4f_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual	N/A	O-SUP-M11S-141019/1109

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
x10dbt-t_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10D-141019/1110
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10D-141019/1111
x10ddw-i_firmware					
Use of Hard-coded	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11	N/A	O-SUP-X10D-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Credentials			products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		141019/1112
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10D-141019/1113
x10ddw-in_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices	N/A	O-SUP-X10D-141019/1114

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10D-141019/1115
x10dgo-t_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10D-141019/1116
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor	N/A	O-SUP-X10D-141019/1117

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		
x10dgq_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10D-141019/1118
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10D-141019/1119
x10drc-ln4+_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10D-141019/1120
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10D-141019/1121
x10drc-t4+_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can	N/A	O-SUP-X10D-141019/1122

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10D-141019/1123
x10drd-i_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10D-141019/1124
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different	N/A	O-SUP-X10D-141019/1125

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		
x10drd-int_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10D-141019/1126
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-X10D-141019/1127

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-16650		
x10drd-intp_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10D-141019/1128
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10D-141019/1129
x10drd-it_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC	N/A	O-SUP-X10D-141019/1130

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10D-141019/1131
x10drd-itp_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10D-141019/1132
Improper	20-09-2019	7.5	On Supermicro X10 and X11	N/A	O-SUP-X10D-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		141019/1133
x10drd-l_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10D-141019/1134
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB	N/A	O-SUP-X10D-141019/1135

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		
x10drd-lt_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10D-141019/1136
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10D-141019/1137
x10drd-ltp_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in	N/A	O-SUP-X10D-141019/1138

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10D-141019/1139
x10drff-c_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-X10D-141019/1140

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-16649		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**	N/A	O-SUP-X10D-141019/1141
x10drff-cg_firmware					
Use of Hard-coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16649**	N/A	O-SUP-X10D-141019/1142
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker	N/A	O-SUP-X10D-141019/1143

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. **CVE ID : CVE-2019-16650**		
telestar					
imperial_i450_firmware					
Improper Authentication	16-09-2019	7.5	TELESTAR Bobs Rock Radio, Dabman D10, Dabman i30 Stereo, Imperial i110, Imperial i150, Imperial i200, Imperial i200-cd, Imperial i400, Imperial i450, Imperial i500-bt, and Imperial i600 TN81HH96-g102h-g102 devices have insufficient access control for the /set_dname, /mylogo, /LocalPlay, /irdevice.xml, /Sendkey, /setvol, /hotkeylist, /init, /playlogo.jpg, /stop, /exit, /back, and /playinfo commands. **CVE ID : CVE-2019-13474**	N/A	O-TEL-IMPE-141019/1144
imperial_i500-bt_firmware					
Improper Authentication	16-09-2019	7.5	TELESTAR Bobs Rock Radio, Dabman D10, Dabman i30 Stereo, Imperial i110, Imperial i150, Imperial i200, Imperial i200-cd, Imperial i400, Imperial i450, Imperial i500-bt, and Imperial i600 TN81HH96-g102h-g102 devices have insufficient access control for the /set_dname, /mylogo, /LocalPlay, /irdevice.xml,	N/A	O-TEL-IMPE-141019/1145

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			/Sendkey, /setvol, /hotkeylist, /init, /playlogo.jpg, /stop, /exit, /back, and /playinfo commands. **CVE ID : CVE-2019-13474**		
bobs_rock_radio_firmware					
Improper Authentication	16-09-2019	7.5	TELESTAR Bobs Rock Radio, Dabman D10, Dabman i30 Stereo, Imperial i110, Imperial i150, Imperial i200, Imperial i200-cd, Imperial i400, Imperial i450, Imperial i500-bt, and Imperial i600 TN81HH96-g102h-g102 devices have insufficient access control for the /set_dname, /mylogo, /LocalPlay, /irdevice.xml, /Sendkey, /setvol, /hotkeylist, /init, /playlogo.jpg, /stop, /exit, /back, and /playinfo commands. **CVE ID : CVE-2019-13474**	N/A	O-TEL-BOBS-141019/1146
dabman_d10_firmware					
Improper Authentication	16-09-2019	7.5	TELESTAR Bobs Rock Radio, Dabman D10, Dabman i30 Stereo, Imperial i110, Imperial i150, Imperial i200, Imperial i200-cd, Imperial i400, Imperial i450, Imperial i500-bt, and Imperial i600 TN81HH96-g102h-g102 devices have insufficient access control for the /set_dname, /mylogo, /LocalPlay, /irdevice.xml, /Sendkey, /setvol,	N/A	O-TEL-DABM-141019/1147

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			/hotkeylist, /init, /playlogo.jpg, /stop, /exit, /back, and /playinfo commands. **CVE ID : CVE-2019-13474**		
dabman_i30_stereo_firmware					
Improper Authentication	16-09-2019	7.5	TELESTAR Bobs Rock Radio, Dabman D10, Dabman i30 Stereo, Imperial i110, Imperial i150, Imperial i200, Imperial i200-cd, Imperial i400, Imperial i450, Imperial i500-bt, and Imperial i600 TN81HH96-g102h-g102 devices have insufficient access control for the /set_dname, /mylogo, /LocalPlay, /irdevice.xml, /Sendkey, /setvol, /hotkeylist, /init, /playlogo.jpg, /stop, /exit, /back, and /playinfo commands. **CVE ID : CVE-2019-13474**	N/A	O-TEL-DABM-141019/1148
imperial_i110_firmware					
Improper Authentication	16-09-2019	7.5	TELESTAR Bobs Rock Radio, Dabman D10, Dabman i30 Stereo, Imperial i110, Imperial i150, Imperial i200, Imperial i200-cd, Imperial i400, Imperial i450, Imperial i500-bt, and Imperial i600 TN81HH96-g102h-g102 devices have insufficient access control for the /set_dname, /mylogo, /LocalPlay, /irdevice.xml, /Sendkey, /setvol, /hotkeylist, /init,	N/A	O-TEL-IMPE-141019/1149

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			/playlogo.jpg, /stop, /exit, /back, and /playinfo commands. **CVE ID : CVE-2019-13474**		
imperial_i150_firmware					
Improper Authentication	16-09-2019	7.5	TELESTAR Bobs Rock Radio, Dabman D10, Dabman i30 Stereo, Imperial i110, Imperial i150, Imperial i200, Imperial i200-cd, Imperial i400, Imperial i450, Imperial i500-bt, and Imperial i600 TN81HH96-g102h-g102 devices have insufficient access control for the /set_dname, /mylogo, /LocalPlay, /irdevice.xml, /Sendkey, /setvol, /hotkeylist, /init, /playlogo.jpg, /stop, /exit, /back, and /playinfo commands. **CVE ID : CVE-2019-13474**	N/A	O-TEL-IMPE-141019/1150
imperial_i200-cd_firmware					
Improper Authentication	16-09-2019	7.5	TELESTAR Bobs Rock Radio, Dabman D10, Dabman i30 Stereo, Imperial i110, Imperial i150, Imperial i200, Imperial i200-cd, Imperial i400, Imperial i450, Imperial i500-bt, and Imperial i600 TN81HH96-g102h-g102 devices have insufficient access control for the /set_dname, /mylogo, /LocalPlay, /irdevice.xml, /Sendkey, /setvol, /hotkeylist, /init, /playlogo.jpg, /stop, /exit,	N/A	O-TEL-IMPE-141019/1151

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			/back, and /playinfo commands. **CVE ID : CVE-2019-13474**		
imperial_i200_firmware					
Improper Authentication	16-09-2019	7.5	TELESTAR Bobs Rock Radio, Dabman D10, Dabman i30 Stereo, Imperial i110, Imperial i150, Imperial i200, Imperial i200-cd, Imperial i400, Imperial i450, Imperial i500-bt, and Imperial i600 TN81HH96-g102h-g102 devices have insufficient access control for the /set_dname, /mylogo, /LocalPlay, /irdevice.xml, /Sendkey, /setvol, /hotkeylist, /init, /playlogo.jpg, /stop, /exit, /back, and /playinfo commands. **CVE ID : CVE-2019-13474**	N/A	O-TEL-IMPE-141019/1152
imperial_i400_firmware					
Improper Authentication	16-09-2019	7.5	TELESTAR Bobs Rock Radio, Dabman D10, Dabman i30 Stereo, Imperial i110, Imperial i150, Imperial i200, Imperial i200-cd, Imperial i400, Imperial i450, Imperial i500-bt, and Imperial i600 TN81HH96-g102h-g102 devices have insufficient access control for the /set_dname, /mylogo, /LocalPlay, /irdevice.xml, /Sendkey, /setvol, /hotkeylist, /init, /playlogo.jpg, /stop, /exit, /back, and /playinfo	N/A	O-TEL-IMPE-141019/1153

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			commands. **CVE ID : CVE-2019-13474**		
imperial_i600_firmware					
Improper Authenticati on	16-09-2019	7.5	TELESTAR Bobs Rock Radio, Dabman D10, Dabman i30 Stereo, Imperial i110, Imperial i150, Imperial i200, Imperial i200-cd, Imperial i400, Imperial i450, Imperial i500-bt, and Imperial i600 TN81HH96-g102h-g102 devices have insufficient access control for the /set_dname, /mylogo, /LocalPlay, /irdevice.xml, /Sendkey, /setvol, /hotkeylist, /init, /playlogo.jpg, /stop, /exit, /back, and /playinfo commands. **CVE ID : CVE-2019-13474**	N/A	O-TEL-IMPE-141019/1154
Tendacn					
n301_firmware					
Improper Input Validation	19-09-2019	7.8	In goform/setSysTools on Tenda N301 wireless routers, attackers can trigger a device crash via a zero wanMTU value. (Prohibition of this zero value is only enforced within the GUI.) **CVE ID : CVE-2019-16412**	N/A	O-TEN-N301-141019/1155
topcon					
net-g5_firmware					
Improper Privilege Management	20-09-2019	6.5	An issue was discovered on Topcon Positioning Net-G5 GNSS Receiver devices with firmware 5.2.2. The web interface of the product is	N/A	O-TOP-NET--141019/1156

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			protected by a login. A guest is allowed to login. Once logged in as a guest, an attacker can browse a URL to read the password of the administrative user. The same procedure allows a regular user to gain administrative privileges. The guest login is possible in the default configuration. **CVE ID : CVE-2019-11326**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	20-09-2019	4	An issue was discovered on Topcon Positioning Net-G5 GNSS Receiver devices with firmware 5.2.2. The web interface of the product has a local file inclusion vulnerability. An attacker with administrative privileges can craft a special URL to read arbitrary files from the device's files system. **CVE ID : CVE-2019-11327**	N/A	O-TOP-NET--141019/1157
Tridium					
niagara4					
Improper Authenticati on	24-09-2019	2.1	A specific utility may allow an attacker to gain read access to privileged files in the Niagara AX 3.8u4 (JACE 3e, JACE 6e, JACE 7, JACE-8000), Niagara 4.4u3 (JACE 3e, JACE 6e, JACE 7, JACE-8000), and Niagara 4.7u1 (JACE-8000, Edge 10). **CVE ID : CVE-2019-13528**	N/A	O-TRI-NIAG-141019/1158
niagara_ax					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	24-09-2019	2.1	A specific utility may allow an attacker to gain read access to privileged files in the Niagara AX 3.8u4 (JACE 3e, JACE 6e, JACE 7, JACE-8000), Niagara 4.4u3 (JACE 3e, JACE 6e, JACE 7, JACE-8000), and Niagara 4.7u1 (JACE-8000, Edge 10). **CVE ID : CVE-2019-13528**	N/A	O-TRI-NIAG-141019/1159
vandyvape					
swell_kit_mod_firmware					
Exposure of Resource to Wrong Sphere	23-09-2019	3.3	An issue was discovered on Swell Kit Mod devices that use the Vandy Vape platform. An attacker may be able to trigger an unintended temperature in the victim's mouth and throat via Bluetooth Low Energy (BLE) packets that specify large power or voltage values. **CVE ID : CVE-2019-16518**	N/A	O-VAN-SWEL-141019/1160
Vmware					
esxi					
Out-of-bounds Read	20-09-2019	5.5	VMware ESXi (6.7 before ESXi670-201904101-SG and 6.5 before ESXi650-201903001), Workstation (15.x before 15.0.3 and 14.x before 14.1.6) and Fusion (11.x before 11.0.3 and 10.x before 10.1.6) contain an out-of-bounds read vulnerability in the pixel shader functionality. Successful exploitation of this issue may lead to	https://www.vmware.com/security/advisories/VMSA-2019-0012.html	O-VMW-ESXI-141019/1161

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information disclosure or may allow attackers with normal user privileges to create a denial-of-service condition on the host. Exploitation of this issue require an attacker to have access to a virtual machine with 3D graphics enabled. It is not enabled by default on ESXi and is enabled by default on Workstation and Fusion. **CVE ID : CVE-2019-5521**		
westerndigital					
wd_my_book_firmware					
Improper Authenticati on	18-09-2019	7.5	Western Digital WD My Book World through II 1.02.12 suffers from Broken Authentication, which allows an attacker to access the /admin/ directory without credentials. An attacker can easily enable SSH from /admin/system_advanced.php?lang=en and login with the default root password welc0me. **CVE ID : CVE-2019-16399**	N/A	O-WES-WD_M-141019/1162
ZTE					
zxv10_b860a_firmware					
Improper Input Validation	23-09-2019	10	All versions up to V81511329.1008 of ZTE ZXV10 B860A products are impacted by input validation vulnerability. Due to input validation, unauthorized users can take advantage of this vulnerability to control	http://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=101	O-ZTE-ZXV1-141019/1163

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the user terminal system. **CVE ID : CVE-2019-3416**	1263	
Hardware					
Schneider-electric					
hmigtu_firmware					
Improper Check for Unusual or Exceptional Conditions	17-09-2019	4.3	A CWE-754 ? Improper Check for Unusual or Exceptional Conditions vulnerability exists in Magelis HMI Panels (all versions of - HMIGTO, HMISTO, XBTGH, HMIGTU, HMIGTUX, HMISCU, HMISTU, XBTGT, XBTGT, HMIGXO, HMIGXU), which could cause a temporary freeze of the HMI when a high rate of frames is received. When the attack stops, the buffered commands are processed by the HMI panel. **CVE ID : CVE-2019-6833**	https://www.schneider-electric.com/ww/en/download/document/SEVD-2019-225-01	H-SCH-HMIG-141019/1164
Vivotek					
camera					
Improper Input Validation	18-09-2019	7.8	VIVOTEK IP Camera devices with firmware before 0x20x allow a denial of service via a crafted HTTP header. **CVE ID : CVE-2019-14458**	N/A	H-VIV-CAME-141019/1165