# National Critical Information Infrastructure Protection Centre

## Common Vulnerabilities and Exposures(CVE) Report

**01 - 15 Oct 2019 Vol. 06 No. 19**

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **Application** | | | | | |
| **activesoft** | | | | | |
| **mybuilder** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 07-10-2019 | 7.5 | ActiveX Control in MyBuilder before 6.2.2019.814 allow an attacker to execute arbitrary command via the ShellOpen method. This can be leveraged for code execution **CVE ID : CVE-2019-12811** | N/A | A-ACT-MYBU-221019/1 |
| Improper Input Validation | 07-10-2019 | 7.5 | MyBuilder viewer before 6.2.2019.814 allow an attacker to execute arbitrary command via specifically crafted configuration file. This can be leveraged for code execution. **CVE ID : CVE-2019-12812** | N/A | A-ACT-MYBU-221019/2 |
| **adhouma_cms_project** | | | | | |
| **adhouma_cms** | | | | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 10-10-2019 | 7.5 | Adhouma CMS through 2019-10-09 has SQL Injection via the post.php p_id parameter. **CVE ID : CVE-2019-17429** | N/A | A-ADH-ADHO-221019/3 |
| **Apache** | | | | | |
| **mina** | | | | | |
| Cleartext | 01-10-2019 | 5 | Handling of the close_notify | N/A | A-APA- |

| 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 |
|---|---|---|---|---|---|
| Transmission of Sensitive Information | | | SSL/TLS message does not lead to a connection closure, leading the server to retain the socket opened and to have the client potentially receive clear text messages afterward. Mitigation: 2.0.20 users should migrate to 2.0.21, 2.1.0 users should migrate to 2.1.1. This issue affects: Apache MINA. **CVE ID : CVE-2019-0231** | | MINA-221019/4 |
| **awplife** | | | | | |
| **contact_form_widget** | | | | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 10-10-2019 | 7.5 | The new-contact-form-widget (aka Contact Form Widget - Contact Query, Form Maker) plugin 1.0.9 for WordPress has SQL Injection via all-query-page.php. **CVE ID : CVE-2019-17072** | N/A | A-AWP-CONT-221019/5 |
| **axiosys** | | | | | |
| **bento4** | | | | | |
| NULL Pointer Dereference | 10-10-2019 | 4.3 | Bento4 1.5.1.0 has a NULL pointer dereference in AP4_DescriptorListInspector::Action in Core/Ap4Descriptor.h, related to AP4_IodsAtom::InspectFields in Core/Ap4IodsAtom.cpp, as demonstrated by mp4dump. **CVE ID : CVE-2019-17452** | N/A | A-AXI-BENT-221019/6 |
| NULL Pointer Dereference | 10-10-2019 | 4.3 | Bento4 1.5.1.0 has a NULL pointer dereference in AP4_DescriptorListWriter::Action in Core/Ap4Descriptor.h, | N/A | A-AXI-BENT-221019/7 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | related to AP4_IodsAtom::WriteFields in Core/Ap4IodsAtom.cpp, as demonstrated by mp4encrypt or mp4compact.<br>**CVE ID : CVE-2019-17453** | | |
| NULL Pointer Dereference | 10-10-2019 | 4.3 | Bento4 1.5.1.0 has a NULL pointer dereference in AP4_Descriptor::GetTag in Core/Ap4Descriptor.h, related to AP4_StsdAtom::GetSampleDescription in Core/Ap4StsdAtom.cpp, as demonstrated by mp4info.<br>**CVE ID : CVE-2019-17454** | N/A | A-AXI-BENT-221019/8 |
| **bludit** | | | | | |
| **bludit** | | | | | |
| Improper Restriction of Excessive Authentication Attempts | 06-10-2019 | 4.3 | bl-kernel/security.class.php in Bludit 3.9.2 allows attackers to bypass a brute-force protection mechanism by using many different forged X-Forwarded-For or Client-IP HTTP headers.<br>**CVE ID : CVE-2019-17240** | N/A | A-BLU-BLUD-221019/9 |
| **bootstrap-3-typeahead_project** | | | | | |
| **bootstrap-3-typeahead** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 08-10-2019 | 4.3 | Bootstrap-3-Typeahead after version 4.0.2 is vulnerable to a cross-site scripting flaw in the highlighter() function. An attacker could exploit this via user interaction to execute code in the user's browser.<br>**CVE ID : CVE-2019-10215** | https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-10215 | A-BOO-BOOT-221019/10 |
| **butor** | | | | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **portal** | | | | | |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 02-10-2019 | 5 | Butor Portal before 1.0.27 is affected by a Path Traversal vulnerability leading to a pre-authentication arbitrary file download. Effectively, a remote anonymous user can download any file on servers running Butor Portal. WhiteLabelingServlet is responsible for this vulnerability. It does not properly sanitize user input on the theme t parameter before reusing it in a path. This path is then used without validation to fetch a file and return its raw content to the user via the /wl?t=../../...&h= substring followed by a filename.<br>**CVE ID : CVE-2019-13343** | https://bitbucket.org/butor-team/portal/commits/all, https://bitbucket.org/butor-team/portal/src/cd7055d33e194fcf530100ee1d8d13aa9cde230b/src/main/java/com/butor/portal/web/servlet/WhiteLabelingServlet.java?at=master | A-BUT-PORT-221019/11 |
| **CA** | | | | | |
| **network_flow_analysis** | | | | | |
| Use of Hard-coded Credentials | 02-10-2019 | 7.5 | CA Network Flow Analysis 9.x and 10.0.x have a default credential vulnerability that can allow a remote attacker to execute arbitrary commands and compromise system security.<br>**CVE ID : CVE-2019-13658** | N/A | A-CA-NETW-221019/12 |
| **Centreon** | | | | | |
| **centreon_vm** | | | | | |
| Reliance on Cookies without | 08-10-2019 | 5 | In Centreon VM through 19.04.3, the cookie configuration within the | N/A | A-CEN-CENT- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Validation and Integrity Checking | | | Apache HTTP Server does not protect against theft because the HTTPOnly flag is not set.<br>**CVE ID : CVE-2019-17104** | | 221019/13 |
| **centreon_web** | | | | | |
| Cleartext Storage of Sensitive Information | 08-10-2019 | 4 | In Centreon Web through 2.8.29, disclosure of external components' passwords allows authenticated attackers to move laterally to external components.<br>**CVE ID : CVE-2019-17106** | N/A | A-CEN-CENT-221019/14 |
| **Checkpoint** | | | | | |
| **security_gateway** | | | | | |
| Improper Handling of Exceptional Conditions | 02-10-2019 | 5 | In a rare scenario, Check Point R80.30 Security Gateway before JHF Take 50 managed by Check Point R80.30 Management crashes with a unique configuration of enhanced logging.<br>**CVE ID : CVE-2019-8462** | N/A | A-CHE-SECU-221019/15 |
| **Cisco** | | | | | |
| **adaptive_security_appliance_software** | | | | | |
| Uncontrolled Resource Consumption | 02-10-2019 | 7.8 | A vulnerability in the Internet Key Exchange version 1 (IKEv1) feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to improper management of system memory. An attacker | N/A | A-CIS-ADAP-221019/16 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | could exploit this vulnerability by sending malicious IKEv1 traffic to an affected device. The attacker does not need valid credentials to authenticate the VPN session, nor does the attacker's source address need to match a peer statement in the crypto map applied to the ingress interface of the affected device. An exploit could allow the attacker to exhaust system memory resources, leading to a reload of an affected device.<br>**CVE ID : CVE-2019-15256** | | |
| **unified_communications_manager** | | | | | |
| Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') | 02-10-2019 | 6.4 | A vulnerability in the web-based interface of Cisco Unified Communications Manager and Cisco Unified Communications Manager Session Management Edition (SME) could allow an unauthenticated, remote attacker to bypass security restrictions. The vulnerability is due to improper handling of malformed HTTP methods. An attacker could exploit this vulnerability by sending a crafted HTTP request to the affected system. A successful exploit could allow the attacker to gain unauthorized access to the system.<br>**CVE ID : CVE-2019-15272** | N/A | A-CIS-UNIF-221019/17 |
| Improper Neutralization of Input | 02-10-2019 | 4.3 | A vulnerability in the web-based interface of multiple Cisco Unified Communications | N/A | A-CIS-UNIF-221019/18 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| During Web Page Generation ('Cross-site Scripting') | | | products could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based interface of the affected software. The vulnerability is due to insufficient validation of user-supplied input by the web-based interface of the affected software. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive browser-based information.<br>**CVE ID : CVE-2019-12707** | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 02-10-2019 | 4 | A vulnerability in the web-based interface of Cisco Unified Communications Manager and Cisco Unified Communications Manager Session Management Edition (SME) could allow an authenticated, remote attacker to impact the confidentiality of an affected system by executing arbitrary SQL queries. The vulnerability exists because the affected software improperly validates user-supplied input in SQL queries. An attacker could exploit this vulnerability by sending crafted requests that contain malicious SQL statements to the affected | N/A | A-CIS-UNIF-221019/19 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | application. A successful exploit could allow the attacker to determine the presence of certain values in the database, impacting the confidentiality of the system.<br>**CVE ID : CVE-2019-12710** | | |
| Improper Restriction of XML External Entity Reference ('XXE') | 02-10-2019 | 6.4 | A vulnerability in the web-based interface of Cisco Unified Communications Manager and Cisco Unified Communications Manager Session Management Edition (SME) could allow an unauthenticated, remote attacker to access sensitive information or cause a denial of service (DoS) condition. The vulnerability is due to improper restrictions on XML entities. An attacker could exploit this vulnerability by sending malicious requests to an affected system that contain references in XML entities. A successful exploit could allow the attacker to retrieve files from the local system, resulting in the disclosure of sensitive information, or cause the application to consume available resources, resulting in a DoS condition.<br>**CVE ID : CVE-2019-12711** | N/A | A-CIS-UNIF-221019/20 |
| Improper Neutralization of Input During Web Page Generation | 02-10-2019 | 4.3 | A vulnerability in the web-based interface of Cisco Unified Communications Manager and Cisco Unified Communications Manager Session Management Edition | N/A | A-CIS-UNIF-221019/21 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ('Cross-site Scripting') | | | (SME) could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based interface of the affected software. The vulnerability is due to insufficient validation of user-supplied input by the web-based interface of the affected software. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive browser-based information.<br>**CVE ID : CVE-2019-12715** | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 02-10-2019 | 4.3 | A vulnerability in the web-based interface of Cisco Unified Communications Manager and Cisco Unified Communications Manager Session Management Edition (SME) could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based interface of the affected software. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. | N/A | A-CIS-UNIF-221019/22 |

| 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 |
|---|---|---|---|---|---|
| | | | A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive browser-based information.<br>**CVE ID : CVE-2019-12716** | | |
| Cross-Site Request Forgery (CSRF) | 02-10-2019 | 4.3 | A vulnerability in the web-based interface of Cisco Unified Communications Manager, Cisco Unified Communications Manager Session Management Edition (SME), Cisco Unified Communications Manager IM and Presence (Unified CM IM&P) Service, and Cisco Unity Connection could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack on an affected system. The vulnerability is due to insufficient CSRF protections by the affected software. An attacker could exploit this vulnerability by persuading a targeted user to click a malicious link. A successful exploit could allow the attacker to send arbitrary requests that could change the password of a targeted user. An attacker could then take unauthorized actions on behalf of the targeted user.<br>**CVE ID : CVE-2019-1915** | N/A | A-CIS-UNIF-221019/23 |
| **firepower_management_center** | | | | | |
| Improper Neutralizatio | 02-10-2019 | 9 | Multiple vulnerabilities in the web-based management | N/A | A-CIS-FIRE- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| n of Special Elements used in an SQL Command ('SQL Injection') | | | interface of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to execute arbitrary SQL injections on an affected device. These vulnerabilities exist due to improper input validation. An attacker could exploit these vulnerabilities by sending crafted SQL queries to an affected device. A successful exploit could allow the attacker to view information that they are not authorized to view, make changes to the system that they are not authorized to make, and execute commands within the underlying operating system that may affect the availability of the device.<br>**CVE ID : CVE-2019-12679** | | 221019/24 |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 02-10-2019 | 9 | Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to execute arbitrary SQL injections on an affected device. These vulnerabilities exist due to improper input validation. An attacker could exploit these vulnerabilities by sending crafted SQL queries to an affected device. A successful exploit could allow the attacker to view information that they are not authorized to view, make changes to the | N/A | A-CIS-FIRE-221019/25 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | system that they are not authorized to make, and execute commands within the underlying operating system that may affect the availability of the device.<br>**CVE ID : CVE-2019-12680** | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 02-10-2019 | 9 | Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to execute arbitrary SQL injections on an affected device. These vulnerabilities exist due to improper input validation. An attacker could exploit these vulnerabilities by sending crafted SQL queries to an affected device. A successful exploit could allow the attacker to view information that they are not authorized to view, make changes to the system that they are not authorized to make, and execute commands within the underlying operating system that may affect the availability of the device.<br>**CVE ID : CVE-2019-12681** | N/A | A-CIS-FIRE-221019/26 |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL | 02-10-2019 | 9 | Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to execute arbitrary SQL injections on an affected | N/A | A-CIS-FIRE-221019/27 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Injection') | | | device. These vulnerabilities exist due to improper input validation. An attacker could exploit these vulnerabilities by sending crafted SQL queries to an affected device. A successful exploit could allow the attacker to view information that they are not authorized to view, make changes to the system that they are not authorized to make, and execute commands within the underlying operating system that may affect the availability of the device.<br>**CVE ID : CVE-2019-12682** | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 02-10-2019 | 9 | Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to execute arbitrary SQL injections on an affected device. These vulnerabilities exist due to improper input validation. An attacker could exploit these vulnerabilities by sending crafted SQL queries to an affected device. A successful exploit could allow the attacker to view information that they are not authorized to view, make changes to the system that they are not authorized to make, and execute commands within the underlying operating system that may affect the availability | N/A | A-CIS-FIRE-221019/28 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | of the device.<br>**CVE ID : CVE-2019-12683** | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 02-10-2019 | 9 | Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to execute arbitrary SQL injections on an affected device. These vulnerabilities exist due to improper input validation. An attacker could exploit these vulnerabilities by sending crafted SQL queries to an affected device. A successful exploit could allow the attacker to view information that they are not authorized to view, make changes to the system that they are not authorized to make, and execute commands within the underlying operating system that may affect the availability of the device.<br>**CVE ID : CVE-2019-12684** | N/A | A-CIS-FIRE-221019/29 |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 02-10-2019 | 9 | Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to execute arbitrary SQL injections on an affected device. These vulnerabilities exist due to improper input validation. An attacker could exploit these vulnerabilities by sending crafted SQL queries to | N/A | A-CIS-FIRE-221019/30 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | an affected device. A successful exploit could allow the attacker to view information that they are not authorized to view, make changes to the system that they are not authorized to make, and execute commands within the underlying operating system that may affect the availability of the device.<br>**CVE ID : CVE-2019-12685** | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 02-10-2019 | 9 | Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to execute arbitrary SQL injections on an affected device. These vulnerabilities exist due to improper input validation. An attacker could exploit these vulnerabilities by sending crafted SQL queries to an affected device. A successful exploit could allow the attacker to view information that they are not authorized to view, make changes to the system that they are not authorized to make, and execute commands within the underlying operating system that may affect the availability of the device.<br>**CVE ID : CVE-2019-12686** | N/A | A-CIS-FIRE-221019/31 |
| Improper Restriction of | 02-10-2019 | 9 | A vulnerability in the web UI of the Cisco Firepower Management Center (FMC) | N/A | A-CIS-FIRE-221019/32 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Operations within the Bounds of a Memory Buffer | | | could allow an authenticated, remote attacker to execute arbitrary commands on an affected device. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to execute arbitrary commands within the affected device.<br>**CVE ID : CVE-2019-12687** | | |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 02-10-2019 | 9 | A vulnerability in the web UI of the Cisco Firepower Management Center (FMC) could allow an authenticated, remote attacker to execute arbitrary commands on an affected device. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to execute arbitrary commands within the affected device.<br>**CVE ID : CVE-2019-12688** | N/A | A-CIS-FIRE-221019/33 |
| Improper Input Validation | 02-10-2019 | 9 | A vulnerability in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to execute arbitrary code on the underlying operating system of an affected device. | N/A | A-CIS-FIRE-221019/34 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending malicious commands to the web-based management interface of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system of the affected device.<br>**CVE ID : CVE-2019-12689** | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 02-10-2019 | 9 | A vulnerability in the web UI of the Cisco Firepower Management Center (FMC) could allow an authenticated, remote attacker to inject arbitrary commands that are executed with the privileges of the root user of the underlying operating system. The vulnerability is due to insufficient validation of user-supplied input to the web UI. An attacker could exploit this vulnerability by submitting crafted input in the web UI. A successful exploit could allow an attacker to execute arbitrary commands on the device with full root privileges.<br>**CVE ID : CVE-2019-12690** | N/A | A-CIS-FIRE-221019/35 |
| Improper Limitation of a Pathname to a Restricted Directory ('Path | 02-10-2019 | 4 | A vulnerability in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to perform a directory | N/A | A-CIS-FIRE-221019/36 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Traversal') | | | traversal attack on an affected device. The vulnerability is due to insufficient input validation by the web-based management interface. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface. A successful exploit could allow the attacker to bypass Cisco FMC Software security restrictions and gain access to the underlying filesystem of the affected device.<br>**CVE ID : CVE-2019-12691** | | |
| Uncontrolled Resource Consumption | 02-10-2019 | 6.8 | A vulnerability in the configuration of the Pluggable Authentication Module (PAM) used in Cisco Firepower Threat Defense (FTD) Software, Cisco Firepower Management Center (FMC) Software, and Cisco FXOS Software could allow an authenticated, remote attacker to cause a denial of service (DoS) condition. The vulnerability is due to improper resource management in the context of user session management. An attacker could exploit this vulnerability by connecting to an affected system and performing many simultaneous successful Secure Shell (SSH) logins. A successful exploit could allow the attacker to exhaust system | N/A | A-CIS-FIRE-221019/37 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | resources and cause the device to reload, resulting in a DoS condition. To exploit this vulnerability, the attacker needs valid user credentials on the system.<br>**CVE ID : CVE-2019-12700** | | |
| Improper Input Validation | 02-10-2019 | 5 | A vulnerability in the file and malware inspection feature of Cisco Firepower Management Center (FMC) Software could allow an unauthenticated, remote attacker to bypass the file and malware inspection policies on an affected system. The vulnerability exists because the affected software insufficiently validates incoming traffic. An attacker could exploit this vulnerability by sending a crafted HTTP request through an affected device. A successful exploit could allow the attacker to bypass the file and malware inspection policies and send malicious traffic through the affected device.<br>**CVE ID : CVE-2019-12701** | N/A | A-CIS-FIRE-221019/38 |
| **prime_infrastructure** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 02-10-2019 | 4.3 | A vulnerability in the web-based management interface of Cisco Prime Infrastructure could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of the affected software. The | N/A | A-CIS-PRIM-221019/39 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | vulnerability is due to insufficient validation of user-supplied input in multiple sections of the web-based management interface of the affected software. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive browser-based information.<br>**CVE ID : CVE-2019-12712** | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 02-10-2019 | 4.3 | A vulnerability in the web-based management interface of Cisco Prime Infrastructure could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of the affected software. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected software. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive browser-based | N/A | A-CIS-PRIM-221019/40 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | information.<br>**CVE ID : CVE-2019-12713** | | |
| **unified_communications_manager_im_and_presence_service** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 02-10-2019 | 4.3 | A vulnerability in the web-based interface of multiple Cisco Unified Communications products could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based interface of the affected software. The vulnerability is due to insufficient validation of user-supplied input by the web-based interface of the affected software. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive browser-based information.<br>**CVE ID : CVE-2019-12707** | N/A | A-CIS-UNIF-221019/41 |
| Cross-Site Request Forgery (CSRF) | 02-10-2019 | 4.3 | A vulnerability in the web-based interface of Cisco Unified Communications Manager, Cisco Unified Communications Manager Session Management Edition (SME), Cisco Unified Communications Manager IM and Presence (Unified CM IM&P) Service, and Cisco Unity Connection could allow an unauthenticated, remote attacker to conduct a cross- | N/A | A-CIS-UNIF-221019/42 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | site request forgery (CSRF) attack on an affected system. The vulnerability is due to insufficient CSRF protections by the affected software. An attacker could exploit this vulnerability by persuading a targeted user to click a malicious link. A successful exploit could allow the attacker to send arbitrary requests that could change the password of a targeted user. An attacker could then take unauthorized actions on behalf of the targeted user.<br>**CVE ID : CVE-2019-1915** | | |
| **adaptive_security_appliance** | | | | | |
| Improper Input Validation | 02-10-2019 | 5 | A vulnerability in the FTP inspection engine of Cisco Adaptive Security (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of FTP data. An attacker could exploit this vulnerability by sending malicious FTP traffic through an affected device. A successful exploit could allow the attacker to cause a DoS condition on the affected device.<br>**CVE ID : CVE-2019-12673** | N/A | A-CIS-ADAP-221019/43 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Input Validation | 02-10-2019 | 3.3 | A vulnerability in the Open Shortest Path First (OSPF) implementation of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability exists because the affected software improperly parses certain options in OSPF link-state advertisement (LSA) type 11 packets. An attacker could exploit this vulnerability by sending a crafted LSA type 11 OSPF packet to an affected device. A successful exploit could allow the attacker to cause a reload of the affected device, resulting in a DoS condition for client traffic that is traversing the device.<br>**CVE ID : CVE-2019-12676** | N/A | A-CIS-ADAP-221019/44 |
| Improper Handling of Exceptional Conditions | 02-10-2019 | 4 | A vulnerability in the Secure Sockets Layer (SSL) VPN feature of Cisco Adaptive Security Appliance (ASA) Software could allow an authenticated, remote attacker to cause a denial of service (DoS) condition that prevents the creation of new SSL/Transport Layer Security (TLS) connections to an affected device. The vulnerability is due to incorrect handling of Base64- | N/A | A-CIS-ADAP-221019/45 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | encoded strings. An attacker could exploit this vulnerability by opening many SSL VPN sessions to an affected device. The attacker would need to have valid user credentials on the affected device to exploit this vulnerability. A successful exploit could allow the attacker to overwrite a special system memory location, which will eventually result in memory allocation errors for new SSL/TLS sessions to the device, preventing successful establishment of these sessions. A reload of the device is required to recover from this condition. Established SSL/TLS connections to the device and SSL/TLS connections through the device are not affected. Note: Although this vulnerability is in the SSL VPN feature, successful exploitation of this vulnerability would affect all new SSL/TLS sessions to the device, including management sessions.<br>**CVE ID : CVE-2019-12677** | | |
| Integer Underflow (Wrap or Wraparound ) | 02-10-2019 | 5 | A vulnerability in the Session Initiation Protocol (SIP) inspection module of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an | N/A | A-CIS-ADAP-221019/46 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | affected device. The vulnerability is due to improper parsing of SIP messages. An attacker could exploit this vulnerability by sending a malicious SIP packet through an affected device. A successful exploit could allow the attacker to trigger an integer underflow, causing the software to try to read unmapped memory and resulting in a crash.<br>**CVE ID : CVE-2019-12678** | | |
| Incorrect Type Conversion or Cast | 02-10-2019 | 4 | A vulnerability in the Secure Copy (SCP) feature of Cisco Adaptive Security Appliance (ASA) Software could allow an authenticated, remote attacker to cause a denial of service (DoS) condition. The vulnerability is due to the use of an incorrect data type for a length variable. An attacker could exploit this vulnerability by initiating the transfer of a large file to an affected device via SCP. To exploit this vulnerability, the attacker would need to have valid privilege level 15 credentials on the affected device. A successful exploit could allow the attacker to cause the length variable to roll over, which could cause the affected device to crash.<br>**CVE ID : CVE-2019-12693** | N/A | A-CIS-ADAP-221019/47 |
| Improper Neutralizatio | 02-10-2019 | 4.3 | A vulnerability in the Clientless SSL VPN (WebVPN) | N/A | A-CIS-ADAP-221019/48 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| n of Input During Web Page Generation ('Cross-site Scripting') | | | portal of Cisco Adaptive Security Appliance (ASA) and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or allow the attacker to access sensitive browser-based information.<br>**CVE ID : CVE-2019-12695** | | |
| Uncontrolled Resource Consumption | 02-10-2019 | 7.8 | A vulnerability in the WebVPN feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause increased CPU utilization on an affected device. The vulnerability is due to excessive processing load for a specific WebVPN HTTP page request. An attacker could exploit this vulnerability by sending multiple WebVPN | N/A | A-CIS-ADAP-221019/49 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | HTTP page load requests for a specific URL. A successful exploit could allow the attacker to increase CPU load on the device, resulting in a denial of service (DoS) condition, which could cause traffic to be delayed through the device.<br>**CVE ID : CVE-2019-12698** | | |
| **firepower_threat_defense** | | | | | |
| Uncontrolled Resource Consumption | 02-10-2019 | 7.8 | A vulnerability in the Internet Key Exchange version 1 (IKEv1) feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to improper management of system memory. An attacker could exploit this vulnerability by sending malicious IKEv1 traffic to an affected device. The attacker does not need valid credentials to authenticate the VPN session, nor does the attacker's source address need to match a peer statement in the crypto map applied to the ingress interface of the affected device. An exploit could allow the attacker to exhaust system memory resources, leading to a reload of an affected device. | N/A | A-CIS-FIRE-221019/50 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2019-15256** | | |
| Improper Input Validation | 02-10-2019 | 5 | A vulnerability in the FTP inspection engine of Cisco Adaptive Security (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of FTP data. An attacker could exploit this vulnerability by sending malicious FTP traffic through an affected device. A successful exploit could allow the attacker to cause a DoS condition on the affected device.<br>**CVE ID : CVE-2019-12673** | N/A | A-CIS-FIRE-221019/51 |
| Improper Encoding or Escaping of Output | 02-10-2019 | 7.2 | Multiple vulnerabilities in the multi-instance feature of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to escape the container for their FTD instance and execute commands with root privileges in the host namespace. These vulnerabilities are due to insufficient protections on the underlying filesystem. An attacker could exploit these vulnerabilities by modifying critical files on the underlying filesystem. A successful exploit could allow the attacker to | N/A | A-CIS-FIRE-221019/52 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | execute commands with root privileges within the host namespace. This could allow the attacker to impact other running FTD instances.<br>**CVE ID : CVE-2019-12674** | | |
| Improper Encoding or Escaping of Output | 02-10-2019 | 7.2 | Multiple vulnerabilities in the multi-instance feature of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to escape the container for their FTD instance and execute commands with root privileges in the host namespace. These vulnerabilities are due to insufficient protections on the underlying filesystem. An attacker could exploit these vulnerabilities by modifying critical files on the underlying filesystem. A successful exploit could allow the attacker to execute commands with root privileges within the host namespace. This could allow the attacker to impact other running FTD instances.<br>**CVE ID : CVE-2019-12675** | N/A | A-CIS-FIRE-221019/53 |
| Improper Input Validation | 02-10-2019 | 3.3 | A vulnerability in the Open Shortest Path First (OSPF) implementation of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a | N/A | A-CIS-FIRE-221019/54 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | denial of service (DoS) condition. The vulnerability exists because the affected software improperly parses certain options in OSPF link-state advertisement (LSA) type 11 packets. An attacker could exploit this vulnerability by sending a crafted LSA type 11 OSPF packet to an affected device. A successful exploit could allow the attacker to cause a reload of the affected device, resulting in a DoS condition for client traffic that is traversing the device.<br>**CVE ID : CVE-2019-12676** | | |
| Integer Underflow (Wrap or Wraparound) | 02-10-2019 | 5 | A vulnerability in the Session Initiation Protocol (SIP) inspection module of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper parsing of SIP messages. An attacker could exploit this vulnerability by sending a malicious SIP packet through an affected device. A successful exploit could allow the attacker to trigger an integer underflow, causing the software to try to read unmapped memory and resulting in a crash. | N/A | A-CIS-FIRE-221019/55 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2019-12678** | | |
| Improper Input Validation | 02-10-2019 | 7.2 | A vulnerability in the command line interface (CLI) of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker with administrative privileges to execute commands on the underlying operating system with root privileges. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by executing a specific CLI command that includes crafted arguments. A successful exploit could allow the attacker to execute commands on the underlying OS with root privileges.<br>**CVE ID : CVE-2019-12694** | N/A | A-CIS-FIRE-221019/56 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 02-10-2019 | 4.3 | A vulnerability in the Clientless SSL VPN (WebVPN) portal of Cisco Adaptive Security Appliance (ASA) and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of an affected device. An attacker could exploit this | N/A | A-CIS-FIRE-221019/57 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or allow the attacker to access sensitive browser-based information.<br>**CVE ID : CVE-2019-12695** | | |
| Uncontrolled Resource Consumption | 02-10-2019 | 7.8 | A vulnerability in the WebVPN feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause increased CPU utilization on an affected device. The vulnerability is due to excessive processing load for a specific WebVPN HTTP page request. An attacker could exploit this vulnerability by sending multiple WebVPN HTTP page load requests for a specific URL. A successful exploit could allow the attacker to increase CPU load on the device, resulting in a denial of service (DoS) condition, which could cause traffic to be delayed through the device.<br>**CVE ID : CVE-2019-12698** | N/A | A-CIS-FIRE-221019/58 |
| Improper Input Validation | 02-10-2019 | 7.2 | Multiple vulnerabilities in the CLI of Cisco FXOS Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local | N/A | A-CIS-FIRE-221019/59 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | attacker to execute commands on the underlying operating system (OS) with root privileges. These vulnerabilities are due to insufficient input validation. An attacker could exploit these vulnerabilities by including crafted arguments to specific CLI commands. A successful exploit could allow the attacker to execute commands on the underlying OS with root privileges.<br>**CVE ID : CVE-2019-12699** | | |
| Uncontrolled Resource Consumption | 02-10-2019 | 6.8 | A vulnerability in the configuration of the Pluggable Authentication Module (PAM) used in Cisco Firepower Threat Defense (FTD) Software, Cisco Firepower Management Center (FMC) Software, and Cisco FXOS Software could allow an authenticated, remote attacker to cause a denial of service (DoS) condition. The vulnerability is due to improper resource management in the context of user session management. An attacker could exploit this vulnerability by connecting to an affected system and performing many simultaneous successful Secure Shell (SSH) logins. A successful exploit could allow the attacker to exhaust system resources and cause the device to reload, resulting in a DoS | N/A | A-CIS-FIRE-221019/60 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | condition. To exploit this vulnerability, the attacker needs valid user credentials on the system.<br>**CVE ID : CVE-2019-12700** | | |
| **identity_services_engine** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 02-10-2019 | 4.3 | A vulnerability in the web-based guest portal of Cisco Identity Services Engine (ISE) could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface. The vulnerability is due to insufficient validation of user-supplied input that is processed by the web-based management interface. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive browser-based information.<br>**CVE ID : CVE-2019-12631** | N/A | A-CIS-IDEN-221019/61 |
| **unity_connection** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 02-10-2019 | 4.3 | A vulnerability in the web-based interface of multiple Cisco Unified Communications products could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based | N/A | A-CIS-UNIT-221019/62 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | based interface of the affected software. The vulnerability is due to insufficient validation of user-supplied input by the web-based interface of the affected software. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive browser-based information.<br>**CVE ID : CVE-2019-12707** | | |
| Cross-Site Request Forgery (CSRF) | 02-10-2019 | 4.3 | A vulnerability in the web-based interface of Cisco Unified Communications Manager, Cisco Unified Communications Manager Session Management Edition (SME), Cisco Unified Communications Manager IM and Presence (Unified CM IM&P) Service, and Cisco Unity Connection could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack on an affected system. The vulnerability is due to insufficient CSRF protections by the affected software. An attacker could exploit this vulnerability by persuading a targeted user to click a malicious link. A successful exploit could allow the attacker to send arbitrary requests that could change the | N/A | A-CIS-UNIT-221019/63 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | password of a targeted user. An attacker could then take unauthorized actions on behalf of the targeted user.<br>**CVE ID : CVE-2019-1915** | | |
| **unified_contact_center_express** | | | | | |
| Improper Input Validation | 02-10-2019 | 4.3 | A vulnerability in Cisco Unified Contact Center Express (UCCX) Software could allow an unauthenticated, remote attacker to conduct an HTTP response splitting attack. The vulnerability is due to insufficient input validation of some parameters that are passed to the web server of the affected system. An attacker could exploit this vulnerability by convincing a user to follow a malicious link or by intercepting a user request on an affected device. A successful exploit could allow the attacker to perform cross-site scripting attacks, web cache poisoning, access sensitive browser-based information, and similar exploits.<br>**CVE ID : CVE-2019-15259** | N/A | A-CIS-UNIF-221019/64 |
| **security_manager** | | | | | |
| Deserialization of Untrusted Data | 02-10-2019 | 7.5 | A vulnerability in the Java deserialization function used by Cisco Security Manager could allow an unauthenticated, remote attacker to execute arbitrary commands on an affected device. The vulnerability is due to insecure deserialization of | N/A | A-CIS-SECU-221019/65 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | user-supplied content by the affected software. An attacker could exploit this vulnerability by sending a malicious serialized Java object to a specific listener on an affected system. A successful exploit could allow the attacker to execute arbitrary commands on the device with the privileges of casuser.<br>**CVE ID : CVE-2019-12630** | | |
| **firepower** | | | | | |
| Improper Input Validation | 02-10-2019 | 5 | Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details section of this advisory.<br>**CVE ID : CVE-2019-12696** | N/A | A-CIS-FIRE-221019/66 |
| Improper Input Validation | 02-10-2019 | 5 | Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details section of this advisory.<br>**CVE ID : CVE-2019-12697** | N/A | A-CIS-FIRE-221019/67 |
| **vdb_fingerprint_database** | | | | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Input Validation | 02-10-2019 | 5 | A vulnerability in the file and malware inspection feature of Cisco Firepower Management Center (FMC) Software could allow an unauthenticated, remote attacker to bypass the file and malware inspection policies on an affected system. The vulnerability exists because the affected software insufficiently validates incoming traffic. An attacker could exploit this vulnerability by sending a crafted HTTP request through an affected device. A successful exploit could allow the attacker to bypass the file and malware inspection policies and send malicious traffic through the affected device. **CVE ID : CVE-2019-12701** | N/A | A-CIS-VDB_-221019/68 |
| **Cmsmadesimple** | | | | | |
| **cms_made_simple** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 06-10-2019 | 3.5 | CMS Made Simple (CMSMS) 2.2.11 allows XSS via the Site Admin > Module Manager > Search Term field. **CVE ID : CVE-2019-17226** | N/A | A-CMS-CMS_-221019/69 |
| **Cpanel** | | | | | |
| **cpanel** | | | | | |
| Insufficient Session Expiration | 09-10-2019 | 6.5 | cPanel before 82.0.15 allows API token credentials to persist after an account has been renamed or terminated (SEC-517). | N/A | A-CPA-CPAN-221019/70 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2019-17375** | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 09-10-2019 | 4.3 | cPanel before 82.0.15 allows self XSS in the SSL Certificate Upload interface (SEC-521).<br>**CVE ID : CVE-2019-17376** | N/A | A-CPA-CPAN-221019/71 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 09-10-2019 | 4.3 | cPanel before 82.0.15 allows self XSS in LiveAPI example scripts (SEC-524).<br>**CVE ID : CVE-2019-17377** | N/A | A-CPA-CPAN-221019/72 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 09-10-2019 | 4.3 | cPanel before 82.0.15 allows self XSS in the SSL Key Delete interface (SEC-526).<br>**CVE ID : CVE-2019-17378** | N/A | A-CPA-CPAN-221019/73 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 09-10-2019 | 4.3 | cPanel before 82.0.15 allows self stored XSS in the WHM SSL Storage Manager interface (SEC-527).<br>**CVE ID : CVE-2019-17379** | N/A | A-CPA-CPAN-221019/74 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site | 09-10-2019 | 4.3 | cPanel before 82.0.15 allows self XSS in the WHM Update Preferences interface (SEC-528).<br>**CVE ID : CVE-2019-17380** | N/A | A-CPA-CPAN-221019/75 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Scripting') | | | | | |
| **Dell** | | | | | |
| **encryption** | | | | | |
| Untrusted Search Path | 07-10-2019 | 6.9 | The vulnerability is limited to the installers of Dell Encryption Enterprise versions prior to 10.4.0 and Dell Endpoint Security Suite Enterprise versions prior to 2.4.0. This issue is exploitable only during the installation of the product by an administrator. A local authenticated low privileged user potentially could exploit this vulnerability by staging a malicious DLL in the search path of the installer prior to its execution by a local administrator. This would cause loading of the malicious DLL, which would allow the attacker to execute arbitrary code in the context of an administrator.<br>**CVE ID : CVE-2019-3745** | N/A | A-DEL-ENCR-221019/76 |
| **endpoint_security_suite_enterprise** | | | | | |
| Untrusted Search Path | 07-10-2019 | 6.9 | The vulnerability is limited to the installers of Dell Encryption Enterprise versions prior to 10.4.0 and Dell Endpoint Security Suite Enterprise versions prior to 2.4.0. This issue is exploitable only during the installation of the product by an administrator. A local authenticated low privileged user potentially could exploit | N/A | A-DEL-ENDP-221019/77 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | this vulnerability by staging a malicious DLL in the search path of the installer prior to its execution by a local administrator. This would cause loading of the malicious DLL, which would allow the attacker to execute arbitrary code in the context of an administrator.<br>**CVE ID : CVE-2019-3745** | | |
| **Elasticsearch** | | | | | |
| **kibana** | | | | | |
| Incorrect Permission Assignment for Critical Resource | 01-10-2019 | 3.5 | A local file disclosure flaw was found in Elastic Code versions 7.3.0, 7.3.1, and 7.3.2. If a malicious code repository is imported into Code it is possible to read arbitrary files from the local filesystem of the Kibana instance running Code with the permission of the Kibana system user.<br>**CVE ID : CVE-2019-7618** | N/A | A-ELA-KIBA-221019/78 |
| **eleopard** | | | | | |
| **animate_it\!** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 09-10-2019 | 4.3 | The animate-it plugin before 2.3.4 for WordPress has XSS.<br>**CVE ID : CVE-2019-17384** | N/A | A-ELE-ANIM-221019/79 |
| Improper Neutralization of Input During Web | 09-10-2019 | 4.3 | The animate-it plugin before 2.3.5 for WordPress has XSS.<br>**CVE ID : CVE-2019-17385** | N/A | A-ELE-ANIM-221019/80 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Page Generation ('Cross-site Scripting') | | | | | |
| **emlog** | | | | | |
| **emlog** | | | | | |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 01-10-2019 | 5.5 | emlog through 6.0.0beta allows remote authenticated users to delete arbitrary files via admin/template.php?action=del&tpl=../ directory traversal.<br>**CVE ID : CVE-2019-17073** | N/A | A-EML-EMLO-221019/81 |
| **enterprisedt** | | | | | |
| **completeftp_server** | | | | | |
| Information Exposure Through Log Files | 02-10-2019 | 3.5 | EnterpriseDT CompleteFTP Server prior to version 12.1.3 is vulnerable to information exposure in the Bootstrap.log file. This allows an attacker to obtain the administrator password hash.<br>**CVE ID : CVE-2019-16116** | N/A | A-ENT-COMP-221019/82 |
| **etoilewebdesign** | | | | | |
| **ultimate_faq** | | | | | |
| Improper Input Validation | 07-10-2019 | 5 | Functions/EWD_UFAQ_Import.php in the ultimate-faqs plugin through 1.8.24 for WordPress allows unauthenticated options import.<br>**CVE ID : CVE-2019-17232** | N/A | A-ETO-ULTI-221019/83 |
| Improper Neutralization of Special Elements in Output Used | 07-10-2019 | 4.3 | Functions/EWD_UFAQ_Import.php in the ultimate-faqs plugin through 1.8.24 for WordPress allows HTML content injection.<br>**CVE ID : CVE-2019-17233** | N/A | A-ETO-ULTI-221019/84 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| by a Downstream Component ('Injection') | | | | | |
| **Exiv2** | | | | | |
| **exiv2** | | | | | |
| Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') | 09-10-2019 | 4.3 | Exiv2 0.27.2 allows attackers to trigger a crash in Exiv2::getULong in types.cpp when called from Exiv2::Internal::CiffDirectory::readDirectory in crwimage_int.cpp, because there is no validation of the relationship of the total size to the offset and size.<br>**CVE ID : CVE-2019-17402** | N/A | A-EXI-EXIV-221019/85 |
| **eyoucms** | | | | | |
| **eyoucms** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 10-10-2019 | 4.3 | EyouCms through 2019-07-11 has XSS related to the login.php web_recordnum parameter.<br>**CVE ID : CVE-2019-17430** | N/A | A-EYO-EYOU-221019/86 |
| **Facebook** | | | | | |
| **hhvm** | | | | | |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 02-10-2019 | 7.5 | Insufficient boundary checks when formatting numbers in number_format allows read/write access to out-of-bounds memory, potentially leading to remote code execution. This issue affects HHVM versions prior to 3.30.10, all versions between | https://github.com/facebook/hhvm/commit/dbeb9a56a638e3fdcef8b691c2a2967132dae692, | A-FAC-HHVM-221019/87 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | 4.0.0 and 4.8.5, all versions between 4.9.0 and 4.18.2, and versions 4.19.0, 4.19.1, 4.20.0, 4.20.1, 4.20.2, 4.21.0, 4.22.0, 4.23.0.<br>**CVE ID : CVE-2019-11929** | https://hhvm.com/blog/2019/09/25/security-update.html, https://www.facebook.com/security/advisories/cve-2019-11929 | |
| **fastadmin** | | | | | |
| **fastadmin** | | | | | |
| Cross-Site Request Forgery (CSRF) | 10-10-2019 | 6.8 | An issue was discovered in fastadmin 1.0.0.20190705_beta. There is a public/index.php/admin/auth/admin/add CSRF vulnerability.<br>**CVE ID : CVE-2019-17431** | N/A | A-FAS-FAST-221019/88 |
| **Fasterxml** | | | | | |
| **jackson-databind** | | | | | |
| Improper Input Validation | 01-10-2019 | 7.5 | A Polymorphic Typing issue was discovered in FasterXML jackson-databind 2.0.0 through 2.9.10. When Default Typing is enabled (either globally or for a specific property) for an externally exposed JSON endpoint and the service has the commons-dbcp (1.4) jar in the classpath, and an attacker can find an RMI service endpoint to access, it is possible to make | N/A | A-FAS-JACK-221019/89 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | the service execute a malicious payload. This issue exists because of org.apache.commons.dbcp.datasources.SharedPoolDataSource and org.apache.commons.dbcp.datasources.PerUserPoolDataSource mishandling.<br>**CVE ID : CVE-2019-16942** | | |
| Improper Input Validation | 01-10-2019 | 7.5 | A Polymorphic Typing issue was discovered in FasterXML jackson-databind 2.0.0 through 2.9.10. When Default Typing is enabled (either globally or for a specific property) for an externally exposed JSON endpoint and the service has the p6spy (3.8.6) jar in the classpath, and an attacker can find an RMI service endpoint to access, it is possible to make the service execute a malicious payload. This issue exists because of com.p6spy.engine.spy.P6DataSource mishandling.<br>**CVE ID : CVE-2019-16943** | N/A | A-FAS-JACK-221019/90 |
| Improper Input Validation | 07-10-2019 | 7.5 | A Polymorphic Typing issue was discovered in FasterXML jackson-databind before 2.9.10. It is related to net.sf.ehcache.hibernate.EhcacheJtaTransactionManagerLookup.<br>**CVE ID : CVE-2019-17267** | N/A | A-FAS-JACK-221019/91 |
| **fecmall** | | | | | |
| **fecmall** | | | | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Unrestricted Upload of File with Dangerous Type | 04-10-2019 | 6.5 | An unrestricted file upload vulnerability was discovered in catalog/productinfo/imageupload in Fecshop FecMall 2.3.4. An attacker can bypass a front-end restriction and upload PHP code to the webserver, by providing image data and the image/jpeg content type, with a .php extension. This occurs because the code relies on the getimagesize function. **CVE ID : CVE-2019-17188** | N/A | A-FEC-FECM-221019/92 |
| **Foxitsoftware** | | | | | |
| **foxit_studio_photo** | | | | | |
| Out-of-bounds Write | 03-10-2019 | 6.8 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Studio Photo 3.6.6.909. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of TIF files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8783. **CVE ID : CVE-2019-13323** | N/A | A-FOX-FOXI-221019/93 |
| Out-of- | 03-10-2019 | 6.8 | This vulnerability allows | N/A | A-FOX-FOXI- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| bounds Read | | | remote attackers to execute arbitrary code on affected installations of Foxit Studio Photo 3.6.6.909. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of TIFF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8782.<br>**CVE ID : CVE-2019-13324** | | 221019/94 |
| Out-of-bounds Read | 03-10-2019 | 6.8 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Studio Photo 3.6.6.909. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of EPS files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI- | N/A | A-FOX-FOXI-221019/95 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | CAN-8922.<br>**CVE ID : CVE-2019-13325** | | |
| **phantompdf** | | | | | |
| Use After Free | 04-10-2019 | 6.8 | This vulnerability allows remote atackers to execute arbitrary code on affected installations of Foxit Reader 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the removeField method. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8656.<br>**CVE ID : CVE-2019-13315** | N/A | A-FOX-PHAN-221019/96 |
| Use After Free | 04-10-2019 | 6.8 | This vulnerability allows remote atackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Calculate actions. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this | N/A | A-FOX-PHAN-221019/97 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | vulnerability to execute code in the context of the current process. Was ZDI-CAN-8757.<br>**CVE ID : CVE-2019-13316** | | |
| Use After Free | 04-10-2019 | 6.8 | This vulnerability allows remote atackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Calculate actions. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8759.<br>**CVE ID : CVE-2019-13317** | N/A | A-FOX-PHAN-221019/98 |
| Use of Externally-Controlled Format String | 04-10-2019 | 4.3 | This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Reader 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of the util.printf Javascript method. The application processes the %p parameter in the format string, allowing | N/A | A-FOX-PHAN-221019/99 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | heap addresses to be returned to the script. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-8544.<br>**CVE ID : CVE-2019-13318** | | |
| Use After Free | 04-10-2019 | 6.8 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of XFA forms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8669.<br>**CVE ID : CVE-2019-13319** | N/A | A-FOX-PHAN-221019/100 |
| Use After Free | 04-10-2019 | 6.8 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of AcroForms. The issue results from the lack of | N/A | A-FOX-PHAN-221019/101 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8814.<br>**CVE ID : CVE-2019-13320** | | |
| Improper Handling of Exceptional Conditions | 02-10-2019 | 6.8 | An exploitable memory corruption vulnerability exists in the JavaScript engine of Foxit Software's Foxit PDF Reader, version 9.4.1.16828. A specially crafted PDF document can trigger an out-of-memory condition which isn't handled properly, resulting in arbitrary code execution. An attacker needs to trick the user to open the malicious file to trigger this vulnerability. If the browser plugin extension is enabled, visiting a malicious site can also trigger the vulnerability.<br>**CVE ID : CVE-2019-5031** | N/A | A-FOX-PHAN-221019/102 |
| Use After Free | 04-10-2019 | 6.8 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.4.1.16828. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the deleteItemAt method when processing AcroForms. The issue results from the lack of validating the existence of an | N/A | A-FOX-PHAN-221019/103 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8295.<br>**CVE ID : CVE-2019-6774** | | |
| Use After Free | 04-10-2019 | 6.8 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the exportValues method within a AcroForm. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8491.<br>**CVE ID : CVE-2019-6775** | N/A | A-FOX-PHAN-221019/104 |
| Use After Free | 04-10-2019 | 6.8 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the removeField method when processing | N/A | A-FOX-PHAN-221019/105 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | watermarks within AcroForms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-8801.<br>**CVE ID : CVE-2019-6776** | | |
| **reader** | | | | | |
| Use After Free | 04-10-2019 | 6.8 | This vulnerability allows remote atackers to execute arbitrary code on affected installations of Foxit Reader 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the removeField method. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8656.<br>**CVE ID : CVE-2019-13315** | N/A | A-FOX-READ-221019/106 |
| Use After Free | 04-10-2019 | 6.8 | This vulnerability allows remote atackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.5.0.20723. User interaction is required to exploit this vulnerability in | N/A | A-FOX-READ-221019/107 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Calculate actions. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8757.<br>**CVE ID : CVE-2019-13316** | | |
| Use After Free | 04-10-2019 | 6.8 | This vulnerability allows remote atackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Calculate actions. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8759.<br>**CVE ID : CVE-2019-13317** | N/A | A-FOX-READ-221019/108 |
| Use of Externally-Controlled Format String | 04-10-2019 | 4.3 | This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Reader 9.5.0.20723. User | N/A | A-FOX-READ-221019/109 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of the util.printf Javascript method. The application processes the %p parameter in the format string, allowing heap addresses to be returned to the script. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-8544.<br>**CVE ID : CVE-2019-13318** | | |
| Use After Free | 04-10-2019 | 6.8 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of XFA forms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8669.<br>**CVE ID : CVE-2019-13319** | N/A | A-FOX-READ-221019/110 |
| Use After Free | 04-10-2019 | 6.8 | This vulnerability allows remote attackers to execute | N/A | A-FOX-READ- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | arbitrary code on affected installations of Foxit Reader 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of AcroForms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8814.<br>**CVE ID : CVE-2019-13320** | | 221019/111 |
| Out-of-bounds Read | 03-10-2019 | 6.8 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of fields within Acroform objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8864.<br>**CVE ID : CVE-2019-13326** | N/A | A-FOX-READ-221019/112 |
| Use After | 03-10-2019 | 6.8 | This vulnerability allows | N/A | A-FOX- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Free | | | remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of fields within Acroform objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8888.<br>**CVE ID : CVE-2019-13327** | | READ-221019/113 |
| Use After Free | 03-10-2019 | 6.8 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of fields within Acroform objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8913. | N/A | A-FOX-READ-221019/114 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2019-13328** | | |
| Access of Resource Using Incompatible Type ('Type Confusion') | 03-10-2019 | 6.8 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.5. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of TIF files. The issue results from the lack of proper validation of user-supplied data, which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8695.<br>**CVE ID : CVE-2019-13329** | N/A | A-FOX-READ-221019/115 |
| Access of Resource Using Incompatible Type ('Type Confusion') | 03-10-2019 | 6.8 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of JPG files. The issue results from the lack of proper validation of user-supplied data, which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8742. | N/A | A-FOX-READ-221019/116 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2019-13330** | | |
| Out-of-bounds Read | 03-10-2019 | 6.8 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JPG files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8838.<br>**CVE ID : CVE-2019-13331** | N/A | A-FOX-READ-221019/117 |
| Use After Free | 03-10-2019 | 6.8 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.6.0.25114. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of templates in XFA forms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of | N/A | A-FOX-READ-221019/118 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | the current process. Was ZDI-CAN-9149.<br>**CVE ID : CVE-2019-13332** | | |
| Missing Release of Resource after Effective Lifetime | 04-10-2019 | 5 | Foxit Reader before 9.7 allows an Access Violation and crash if insufficient memory exists.<br>**CVE ID : CVE-2019-17183** | N/A | A-FOX-READ-221019/119 |
| Improper Handling of Exceptional Conditions | 02-10-2019 | 6.8 | An exploitable memory corruption vulnerability exists in the JavaScript engine of Foxit Software's Foxit PDF Reader, version 9.4.1.16828. A specially crafted PDF document can trigger an out-of-memory condition which isn't handled properly, resulting in arbitrary code execution. An attacker needs to trick the user to open the malicious file to trigger this vulnerability. If the browser plugin extension is enabled, visiting a malicious site can also trigger the vulnerability.<br>**CVE ID : CVE-2019-5031** | N/A | A-FOX-READ-221019/120 |
| Use After Free | 04-10-2019 | 6.8 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.4.1.16828. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the deleteItemAt method when processing AcroForms. The issue results from the lack of | N/A | A-FOX-READ-221019/121 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8295.<br>**CVE ID : CVE-2019-6774** | | |
| Use After Free | 04-10-2019 | 6.8 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the exportValues method within a AcroForm. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8491.<br>**CVE ID : CVE-2019-6775** | N/A | A-FOX-READ-221019/122 |
| Use After Free | 04-10-2019 | 6.8 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the removeField | N/A | A-FOX-READ-221019/123 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | method when processing watermarks within AcroForms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-8801.<br>**CVE ID : CVE-2019-6776** | | |
| **freerdp** | | | | | |
| **freerdp** | | | | | |
| Missing Release of Resource after Effective Lifetime | 04-10-2019 | 5 | libfreerdp/codec/region.c in FreeRDP through 1.1.x and 2.x through 2.0.0-rc4 has memory leaks because a supplied realloc pointer (i.e., the first argument to realloc) is also used for a realloc return value.<br>**CVE ID : CVE-2019-17177** | N/A | A-FRE-FREE-221019/124 |
| Missing Release of Resource after Effective Lifetime | 04-10-2019 | 5 | HuffmanTree_makeFromFrequencies in lodepng.c in LodePNG through 2019-09-28, as used in WinPR in FreeRDP and other products, has a memory leak because a supplied realloc pointer (i.e., the first argument to realloc) is also used for a realloc return value.<br>**CVE ID : CVE-2019-17178** | N/A | A-FRE-FREE-221019/125 |
| **frostming** | | | | | |
| **redis_wrapper** | | | | | |
| Deserialization of | 05-10-2019 | 7.5 | Uncontrolled deserialization of a pickled object in models.py | N/A | A-FRO-REDI-221019/126 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Untrusted Data | | | in Frost Ming rediswrapper (aka Redis Wrapper) before 0.3.0 allows attackers to execute arbitrary scripts.<br>**CVE ID : CVE-2019-17206** | | |
| **glyphandcog** | | | | | |
| **xpdfreader** | | | | | |
| NULL Pointer Dereference | 01-10-2019 | 4.3 | Catalog.cc in Xpdf 4.02 has a NULL pointer dereference because Catalog.pageLabels is initialized too late in the Catalog constructor.<br>**CVE ID : CVE-2019-17064** | N/A | A-GLY-XPDF-221019/127 |
| **Gnome** | | | | | |
| **libsoup** | | | | | |
| Out-of-bounds Read | 06-10-2019 | 7.5 | libsoup from versions 2.65.1 until 2.68.1 have a heap-based buffer over-read because soup_ntlm_parse_challenge() in soup-auth-ntlm.c does not properly check an NTLM message's length before proceeding with a memcpy.<br>**CVE ID : CVE-2019-17266** | N/A | A-GNO-LIBS-221019/128 |
| **gonitro** | | | | | |
| **nitropdf** | | | | | |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 09-10-2019 | 6.8 | A specifically crafted jpeg2000 file embedded in a PDF file can lead to a heap corruption when opening a PDF document in NitroPDF 12.12.1.522. With careful memory manipulation, this can lead to arbitrary code execution. In order to trigger this vulnerability, the victim would need to open the malicious file. | N/A | A-GON-NITR-221019/129 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2019-5045** | | |
| Out-of-bounds Write | 09-10-2019 | 6.8 | A specifically crafted jpeg2000 file embedded in a PDF file can lead to a heap corruption when opening a PDF document in NitroPDF 12.12.1.522. With careful memory manipulation, this can lead to arbitrary code execution. In order to trigger this vulnerability, the victim would need to open the malicious file.<br>**CVE ID : CVE-2019-5046** | N/A | A-GON-NITR-221019/130 |
| Use After Free | 09-10-2019 | 6.8 | An exploitable Use After Free vulnerability exists in the CharProcs parsing functionality of NitroPDF. A specially crafted PDF can cause a type confusion, resulting in a Use After Free. An attacker can craft a malicious PDF to trigger this vulnerability.<br>**CVE ID : CVE-2019-5047** | N/A | A-GON-NITR-221019/131 |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 09-10-2019 | 6.8 | A specifically crafted PDF file can lead to a heap corruption when opened in NitroPDF 12.12.1.522. With careful memory manipulation, this can lead to arbitrary code execution. In order to trigger this vulnerability, the victim would need to open the malicious file.<br>**CVE ID : CVE-2019-5048** | N/A | A-GON-NITR-221019/132 |
| Improper Restriction of Operations | 09-10-2019 | 6.8 | A specifically crafted PDF file can lead to a heap corruption when opened in NitroPDF 12.12.1.522. With careful | N/A | A-GON-NITR-221019/133 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| within the Bounds of a Memory Buffer | | | memory manipulation, this can lead to arbitrary code execution. In order to trigger this vulnerability, the victim would need to open the malicious file.<br>**CVE ID : CVE-2019-5050** | | |
| Incorrect Type Conversion or Cast | 09-10-2019 | 6.8 | An exploitable use-after-free vulnerability exists in the Length parsing function of NitroPDF. A specially crafted PDF can cause a type confusion, resulting in a use-after-free condition. An attacker can craft a malicious PDF to trigger this vulnerability.<br>**CVE ID : CVE-2019-5053** | N/A | A-GON-NITR-221019/134 |
| **HP** | | | | | |
| **arcsight_logger** | | | | | |
| Unrestricted Upload of File with Dangerous Type | 04-10-2019 | 6.5 | Unrestricted file upload vulnerability in Micro Focus ArcSight Logger, version 6.7.0 and later. This vulnerability could allow Unrestricted Upload of File with Dangerous type.<br>**CVE ID : CVE-2019-11655** | N/A | A-HP-ARCS-221019/135 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 04-10-2019 | 3.5 | Stored XSS vulnerability in Micro Focus ArcSight Logger, affects versions prior to Logger 6.7.1 HotFix 6.7.1.8262.0. This vulnerability could allow Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting').<br>**CVE ID : CVE-2019-11656** | N/A | A-HP-ARCS-221019/136 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **hrworks** | | | | | |
| **hrworks** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 08-10-2019 | 3.5 | HRworks 3.36.9 allows XSS via the purpose of a travel-expense report. **CVE ID : CVE-2019-16416** | N/A | A-HRW-HRWO-221019/137 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 08-10-2019 | 3.5 | HRworks FLOW 3.36.9 allows XSS via the purpose of a travel-expense report. **CVE ID : CVE-2019-16417** | N/A | A-HRW-HRWO-221019/138 |
| **IBM** | | | | | |
| **jazz_reporting_service** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 01-10-2019 | 3.5 | IBM Jazz Reporting Service (JRS) 6.0, 6.0.1, 6.0.2, 6.0.3, 6.0.4, 6.0.5, 6.0.6, and 6.0.6.1 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: 164115. **CVE ID : CVE-2019-4494** | https://www.ibm.com/support/pages/node/1074690 | A-IBM-JAZZ-221019/139 |
| Improper Neutralization of Input During Web Page | 01-10-2019 | 3.5 | IBM Jazz Reporting Service (JRS) 6.0, 6.0.1, 6.0.2, 6.0.3, 6.0.4, 6.0.5, 6.0.6, and 6.0.6.1 is vulnerable to cross-site scripting. This vulnerability | https://www.ibm.com/support/pages/node/107469 | A-IBM-JAZZ-221019/140 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Generation ('Cross-site Scripting') | | | 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: 164116.<br>**CVE ID : CVE-2019-4495** | 0 | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 01-10-2019 | 3.5 | IBM Jazz Reporting Service (JRS) 6.0, 6.0.1, 6.0.2, 6.0.3, 6.0.4, 6.0.5, 6.0.6, and 6.0.6.1 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: 164118.<br>**CVE ID : CVE-2019-4497** | https://www.ibm.com/support/pages/node/1074690 | A-IBM-JAZZ-221019/141 |
| **spectrum_scale** | | | | | |
| Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') | 09-10-2019 | 7.2 | A security vulnerability has been identified in all levels of IBM Spectrum Scale V5.0.0.0 through V5.0.3.2 and IBM Spectrum Scale V4.2.0.0 through V4.2.3.17 that could allow a local attacker to obtain root privilege by injecting parameters into setuid files.<br>**CVE ID : CVE-2019-4558** | https://www.ibm.com/support/pages/node/1073732 | A-IBM-SPEC-221019/142 |
| **mq** | | | | | |
| Session Fixation | 04-10-2019 | 7.5 | IBM MQ 8.0.0.4 - 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 AMQP Listeners could allow an | https://www.ibm.com/support/pages/no | A-IBM-MQ-221019/143 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | unauthorized user to conduct a session fixation attack due to clients not being disconnected as they should. IBM X-Force ID: 159352.<br>**CVE ID : CVE-2019-4227** | de/886899 | |
| **daeja_viewone** | | | | | |
| Information Exposure | 01-10-2019 | 5 | IBM Daeja ViewONE Virtual 5.0 through 5.0.6 could expose internal parameters to ViewONE clients that could be used in further attacks against the system. IBM X-Force ID: 159521.<br>**CVE ID : CVE-2019-4246** | https://www.ibm.com/support/pages/node/884380 | A-IBM-DAEJ-221019/144 |
| **maximo_anywhere** | | | | | |
| Insecure Storage of Sensitive Information | 10-10-2019 | 2.1 | IBM Maximo Anywhere 7.6.0, 7.6.1, 7.6.2, and 7.6.3 does not have device root detection which could result in an attacker gaining sensitive information about the device. IBM X-Force ID: 160198.<br>**CVE ID : CVE-2019-4265** | https://www.ibm.com/support/pages/node/1078995 | A-IBM-MAXI-221019/145 |
| **security_guardium** | | | | | |
| Improper Authentication | 03-10-2019 | 6.5 | IBM Security Guardium 9.0, 9.5, and 10.6 are vulnerable to a privilege escalation which could allow an authenticated user to change the accessmgr password. IBM X-Force ID: 162768.<br>**CVE ID : CVE-2019-4422** | https://supportcontent.ibm.com/support/pages/node/957491 | A-IBM-SECU-221019/146 |
| **security_key_lifecycle_manager** | | | | | |
| Incorrect Authorization | 04-10-2019 | 5 | IBM Security Key Lifecycle Manager 2.6, 2.7, 3.0, and 3.0.1 discloses sensitive information | https://www.ibm.com/support | A-IBM-SECU-221019/147 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | to unauthorized users. The information can be used to mount further attacks on the system. IBM X-Force ID: 165136.<br>**CVE ID : CVE-2019-4514** | /pages/node/302017 | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 04-10-2019 | 4.3 | IBM Security Key Lifecycle Manager 2.6, 2.7, 3.0, and 3.0.1 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.<br>**CVE ID : CVE-2019-4564** | https://www.ibm.com/support/pages/node/302001 | A-IBM-SECU-221019/148 |
| **security_directory_server** | | | | | |
| Improper Restriction of Excessive Authentication Attempts | 02-10-2019 | 5 | IBM Security Directory Server 6.4.0 uses an inadequate account lockout setting that could allow a remote attacker to brute force account credentials. IBM X-Force ID: 165178.<br>**CVE ID : CVE-2019-4520** | https://www.ibm.com/support/pages/node/1077045 | A-IBM-SECU-221019/149 |
| URL Redirection to Untrusted Site ('Open Redirect') | 02-10-2019 | 5.8 | IBM Security Directory Server 6.4.0 could allow a remote attacker to conduct phishing attacks, using an open redirect attack. By persuading a victim to visit a specially-crafted Web site, a remote attacker could exploit this vulnerability to spoof the URL displayed to redirect a user to a malicious Web site that would appear to be trusted. This could allow | https://www.ibm.com/support/pages/node/1077045 | A-IBM-SECU-221019/150 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | the attacker to obtain highly sensitive information or conduct further attacks against the victim. IBM X-Force ID: 165660.<br>**CVE ID : CVE-2019-4538** | | |
| XML Injection (aka Blind XPath Injection) | 02-10-2019 | 5.5 | IBM Security Directory Server 6.4.0 does not properly neutralize special elements that are used in XML, allowing attackers to modify the syntax, content, or commands of the XML before it is processed by an end system. IBM X-Force ID: 165812.<br>**CVE ID : CVE-2019-4539** | https://www.ibm.com/support/pages/node/1077045 | A-IBM-SECU-221019/151 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 02-10-2019 | 4.3 | IBM Security Directory Server 6.4.0 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: 165815.<br>**CVE ID : CVE-2019-4542** | https://www.ibm.com/support/pages/node/1077045 | A-IBM-SECU-221019/152 |
| Insecure Storage of Sensitive Information | 02-10-2019 | 5 | IBM Security Directory Server 6.4.0 discloses sensitive information to unauthorized users. The information can be used to mount further attacks on the system. IBM X-Force ID: 165951.<br>**CVE ID : CVE-2019-4549** | https://www.ibm.com/support/pages/node/1077045 | A-IBM-SECU-221019/153 |
| **websphere_application_server** | | | | | |
| Information | 03-10-2019 | 5 | IBM WebSphere Application | https://w | A-IBM- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Exposure Through an Error Message | | | Server 7.0, 8.0, 8.5, 9.0, and Liberty could allow a remote attacker to obtain sensitive information when a stack trace is returned in the browser. IBM X-Force ID: 163177. **CVE ID : CVE-2019-4441** | ww.ibm.com/support/pages/node/959023 | WEBS-221019/154 |
| **control_desk** | | | | | |
| Information Exposure Through an Error Message | 09-10-2019 | 4 | IBM Maximo Asset Management 7.6.1.1 generates an error message that includes sensitive information that could be used in further attacks against the system. IBM X-Force ID: 164554. **CVE ID : CVE-2019-4512** | https://www.ibm.com/support/pages/node/1075413 | A-IBM-CONT-221019/155 |
| **maximo_asset_management** | | | | | |
| Information Exposure Through an Error Message | 09-10-2019 | 4 | IBM Maximo Asset Management 7.6.1.1 generates an error message that includes sensitive information that could be used in further attacks against the system. IBM X-Force ID: 164554. **CVE ID : CVE-2019-4512** | https://www.ibm.com/support/pages/node/1075413 | A-IBM-MAXI-221019/156 |
| **maximo_for_aviation** | | | | | |
| Information Exposure Through an Error Message | 09-10-2019 | 4 | IBM Maximo Asset Management 7.6.1.1 generates an error message that includes sensitive information that could be used in further attacks against the system. IBM X-Force ID: 164554. **CVE ID : CVE-2019-4512** | https://www.ibm.com/support/pages/node/1075413 | A-IBM-MAXI-221019/157 |
| **maximo_for_life_sciences** | | | | | |
| Information Exposure | 09-10-2019 | 4 | IBM Maximo Asset Management 7.6.1.1 generates | https://www.ibm.co | A-IBM-MAXI- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Through an Error Message | | | an error message that includes sensitive information that could be used in further attacks against the system. IBM X-Force ID: 164554.<br>**CVE ID : CVE-2019-4512** | m/support/pages/node/1075413 | 221019/158 |
| **maximo_for_nuclear_power** | | | | | |
| Information Exposure Through an Error Message | 09-10-2019 | 4 | IBM Maximo Asset Management 7.6.1.1 generates an error message that includes sensitive information that could be used in further attacks against the system. IBM X-Force ID: 164554.<br>**CVE ID : CVE-2019-4512** | https://www.ibm.com/support/pages/node/1075413 | A-IBM-MAXI-221019/159 |
| **maximo_for_oil_and_gas** | | | | | |
| Information Exposure Through an Error Message | 09-10-2019 | 4 | IBM Maximo Asset Management 7.6.1.1 generates an error message that includes sensitive information that could be used in further attacks against the system. IBM X-Force ID: 164554.<br>**CVE ID : CVE-2019-4512** | https://www.ibm.com/support/pages/node/1075413 | A-IBM-MAXI-221019/160 |
| **maximo_for_transportation** | | | | | |
| Information Exposure Through an Error Message | 09-10-2019 | 4 | IBM Maximo Asset Management 7.6.1.1 generates an error message that includes sensitive information that could be used in further attacks against the system. IBM X-Force ID: 164554.<br>**CVE ID : CVE-2019-4512** | https://www.ibm.com/support/pages/node/1075413 | A-IBM-MAXI-221019/161 |
| **maximo_for_utilities** | | | | | |
| Information Exposure Through an | 09-10-2019 | 4 | IBM Maximo Asset Management 7.6.1.1 generates an error message that includes | https://www.ibm.com/support | A-IBM-MAXI-221019/162 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Error Message | | | sensitive information that could be used in further attacks against the system. IBM X-Force ID: 164554.<br>**CVE ID : CVE-2019-4512** | /pages/node/1075413 | |
| **smartcloud_control_desk** | | | | | |
| Information Exposure Through an Error Message | 09-10-2019 | 4 | IBM Maximo Asset Management 7.6.1.1 generates an error message that includes sensitive information that could be used in further attacks against the system. IBM X-Force ID: 164554.<br>**CVE ID : CVE-2019-4512** | https://www.ibm.com/support/pages/node/1075413 | A-IBM-SMAR-221019/163 |
| **tivoli_integration_composer** | | | | | |
| Information Exposure Through an Error Message | 09-10-2019 | 4 | IBM Maximo Asset Management 7.6.1.1 generates an error message that includes sensitive information that could be used in further attacks against the system. IBM X-Force ID: 164554.<br>**CVE ID : CVE-2019-4512** | https://www.ibm.com/support/pages/node/1075413 | A-IBM-TIVO-221019/164 |
| **intelliantech** | | | | | |
| **remote_access** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 07-10-2019 | 10 | Intellian Remote Access 3.18 allows remote attackers to execute arbitrary OS commands via shell metacharacters in the Ping Test field.<br>**CVE ID : CVE-2019-17269** | N/A | A-INT-REMO-221019/165 |
| **Intelliants** | | | | | |
| **subrion** | | | | | |
| Improper | 06-10-2019 | 3.5 | Subrion 4.2.1 allows XSS via | N/A | A-INT-SUBR- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Neutralization of Input During Web Page Generation ('Cross-site Scripting') | | | the panel/members/ Username, Full Name, or Email field, aka an "Admin Member JSON Update" issue.<br>**CVE ID : CVE-2019-17225** | | 221019/166 |
| **Irfanview** | | | | | |
| **irfanview** | | | | | |
| Out-of-bounds Write | 08-10-2019 | 4.6 | IrfanView 4.53 allows a User Mode Write AV starting at WSQ!ReadWSQ+0x000000000000d563.<br>**CVE ID : CVE-2019-17241** | N/A | A-IRF-IRFA-221019/167 |
| Out-of-bounds Write | 08-10-2019 | 4.6 | IrfanView 4.53 allows a User Mode Write AV starting at WSQ!ReadWSQ+0x000000000000966f.<br>**CVE ID : CVE-2019-17242** | N/A | A-IRF-IRFA-221019/168 |
| Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') | 08-10-2019 | 6.8 | IrfanView 4.53 allows Data from a Faulting Address to control Code Flow starting at JPEG_LS+0x0000000000003155.<br>**CVE ID : CVE-2019-17243** | N/A | A-IRF-IRFA-221019/169 |
| Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') | 08-10-2019 | 6.8 | IrfanView 4.53 allows Data from a Faulting Address to control Code Flow starting at JPEG_LS+0x0000000000001d8a.<br>**CVE ID : CVE-2019-17244** | N/A | A-IRF-IRFA-221019/170 |
| Out-of-bounds Write | 08-10-2019 | 4.6 | IrfanView 4.53 allows a User Mode Write AV starting at WSQ!ReadWSQ+0x000000000004359.<br>**CVE ID : CVE-2019-17245** | N/A | A-IRF-IRFA-221019/171 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Out-of-bounds Write | 08-10-2019 | 6.8 | IrfanView 4.53 allows a User Mode Write AV starting at WSQ!ReadWSQ+0x000000000000258c. **CVE ID : CVE-2019-17246** | N/A | A-IRF-IRFA-221019/172 |
| Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') | 08-10-2019 | 6.8 | IrfanView 4.53 allows Data from a Faulting Address to control a subsequent Write Address starting at JPEG_LS+0x0000000000007da8. **CVE ID : CVE-2019-17247** | N/A | A-IRF-IRFA-221019/173 |
| Out-of-bounds Write | 08-10-2019 | 6.8 | IrfanView 4.53 allows a User Mode Write AV starting at WSQ!ReadWSQ+0x00000000000025b6. **CVE ID : CVE-2019-17248** | N/A | A-IRF-IRFA-221019/174 |
| Out-of-bounds Write | 08-10-2019 | 6.8 | IrfanView 4.53 allows a User Mode Write AV starting at WSQ!ReadWSQ+0x00000000000d57b. **CVE ID : CVE-2019-17249** | N/A | A-IRF-IRFA-221019/175 |
| Out-of-bounds Write | 08-10-2019 | 6.8 | IrfanView 4.53 allows a User Mode Write AV starting at WSQ!ReadWSQ+0x00000000000042f5. **CVE ID : CVE-2019-17250** | N/A | A-IRF-IRFA-221019/176 |
| Out-of-bounds Write | 08-10-2019 | 6.8 | IrfanView 4.53 allows a User Mode Write AV starting at FORMATS!GetPlugInInfo+0x0000000000007d43. **CVE ID : CVE-2019-17251** | N/A | A-IRF-IRFA-221019/177 |
| Out-of-bounds Write | 08-10-2019 | 6.8 | IrfanView 4.53 allows a User Mode Write AV starting at FORMATS!Read_BadPNG+0x0000000000000115. **CVE ID : CVE-2019-17252** | N/A | A-IRF-IRFA-221019/178 |

| 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 |
|---|---|---|---|---|---|
| Out-of-bounds Write | 08-10-2019 | 6.8 | IrfanView 4.53 allows a User Mode Write AV starting at JPEG_LS+0x000000000000a6b8. **CVE ID : CVE-2019-17253** | N/A | A-IRF-IRFA-221019/179 |
| Out-of-bounds Write | 08-10-2019 | 6.8 | IrfanView 4.53 allows Data from a Faulting Address to control a subsequent Write Address starting at FORMATS!Read_BadPNG+0x0000000000000101. **CVE ID : CVE-2019-17254** | N/A | A-IRF-IRFA-221019/180 |
| Out-of-bounds Write | 08-10-2019 | 6.8 | IrfanView 4.53 allows a User Mode Write AV starting at EXR!ReadEXR+0x0000000000010836. **CVE ID : CVE-2019-17255** | N/A | A-IRF-IRFA-221019/181 |
| Out-of-bounds Write | 08-10-2019 | 6.8 | IrfanView 4.53 allows a User Mode Write AV starting at DPX!ReadDPX_W+0x00000000000001203. **CVE ID : CVE-2019-17256** | N/A | A-IRF-IRFA-221019/182 |
| Improper Check for Unusual or Exceptional Conditions | 08-10-2019 | 4.3 | IrfanView 4.53 allows a Exception Handler Chain to be Corrupted starting at EXR!ReadEXR+0x0000000000002af80. **CVE ID : CVE-2019-17257** | N/A | A-IRF-IRFA-221019/183 |
| Out-of-bounds Write | 08-10-2019 | 6.8 | IrfanView 4.53 allows Data from a Faulting Address to control a subsequent Write Address starting at JPEG_LS+0x000000000000839c. **CVE ID : CVE-2019-17258** | N/A | A-IRF-IRFA-221019/184 |
| **Jenkins** | | | | | |
| **html_publisher** | | | | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 01-10-2019 | 3.5 | Jenkins HTML Publisher Plugin 1.20 and earlier did not escape the project and build display names in the HTML report frame, resulting in a cross-site scripting vulnerability exploitable by users able to change those. **CVE ID : CVE-2019-10432** | https://jenkins.io/security/advisory/2019-10-01/#SECURITY-1590 | A-JEN-HTML-221019/185 |
| **dingding** | | | | | |
| Cleartext Storage of Sensitive Information | 01-10-2019 | 2.1 | Jenkins Dingding[??] 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-2019-10433** | https://jenkins.io/security/advisory/2019-10-01/#SECURITY-1423 | A-JEN-DING-221019/186 |
| **ldap_email** | | | | | |
| Cleartext Transmission of Sensitive Information | 01-10-2019 | 5 | Jenkins LDAP Email Plugin transmits configured credentials in plain text as part of the global Jenkins configuration form, potentially resulting in their exposure. **CVE ID : CVE-2019-10434** | https://jenkins.io/security/advisory/2019-10-01/#SECURITY-1515 | A-JEN-LDAP-221019/187 |
| **sourcegear_vault** | | | | | |
| Cleartext Transmission of Sensitive Information | 01-10-2019 | 5 | Jenkins SourceGear Vault Plugin transmits configured credentials in plain text as part of job configuration forms, potentially resulting in their exposure. **CVE ID : CVE-2019-10435** | https://jenkins.io/security/advisory/2019-10-01/#SECURITY-1524 | A-JEN-SOUR-221019/188 |
| **script_security** | | | | | |
| Improper | 01-10-2019 | 6.5 | A sandbox bypass | https://jen | A-JEN-SCRI- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Control of Generation of Code ('Code Injection') | | | vulnerability in Jenkins Script Security Plugin 1.64 and earlier related to the handling of default parameter expressions in constructors allowed attackers to execute arbitrary code in sandboxed scripts.<br>**CVE ID : CVE-2019-10431** | kins.io/security/advisory/2019-10-01/#SECURITY-1579 | 221019/189 |
| **Jetbrains** | | | | | |
| **intellij_idea** | | | | | |
| Missing Encryption of Sensitive Data | 01-10-2019 | 4.3 | JetBrains IntelliJ IDEA before 2019.2 was resolving the markdown plantuml artifact download link via a cleartext http connection.<br>**CVE ID : CVE-2019-14954** | https://blog.jetbrains.com/blog/2019/09/26/jetbrains-security-bulletin-q2-2019/ | A-JET-INTE-221019/190 |
| **upsource** | | | | | |
| Information Exposure Through an Error Message | 02-10-2019 | 5 | Server metadata could be exposed because one of the error messages reflected the whole response back to the client in JetBrains TeamCity versions before 2018.2.5 and UpSource versions before 2018.2 build 1293.<br>**CVE ID : CVE-2019-12156** | https://blog.jetbrains.com/blog/2019/09/26/jetbrains-security-bulletin-q2-2019/ | A-JET-UPSO-221019/191 |
| Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') | 02-10-2019 | 10 | In JetBrains TeamCity versions before 2018.2.5 and UpSource versions before 2018.2 build 1293, improper validation of user input for one of the fields could lead to Command Injection.<br>**CVE ID : CVE-2019-12157** | N/A | A-JET-UPSO-221019/192 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 01-10-2019 | 4.3 | JetBrains Upsource before 2019.1.1412 was not properly escaping HTML tags in a code block comments, leading to XSS.<br>**CVE ID : CVE-2019-14961** | N/A | A-JET-UPSO-221019/193 |
| **teamcity** | | | | | |
| Information Exposure Through an Error Message | 02-10-2019 | 5 | Server metadata could be exposed because one of the error messages reflected the whole response back to the client in JetBrains TeamCity versions before 2018.2.5 and UpSource versions before 2018.2 build 1293.<br>**CVE ID : CVE-2019-12156** | https://blog.jetbrains.com/blog/2019/09/26/jetbrains-security-bulletin-q2-2019/ | A-JET-TEAM-221019/194 |
| Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') | 02-10-2019 | 10 | In JetBrains TeamCity versions before 2018.2.5 and UpSource versions before 2018.2 build 1293, improper validation of user input for one of the fields could lead to Command Injection.<br>**CVE ID : CVE-2019-12157** | N/A | A-JET-TEAM-221019/195 |
| Information Exposure | 01-10-2019 | 4 | An issue was discovered in JetBrains TeamCity 2018.2.4. A TeamCity Project administrator could get access to potentially confidential server-level data. The issue was fixed in TeamCity 2018.2.5 and 2019.1.<br>**CVE ID : CVE-2019-15035** | N/A | A-JET-TEAM-221019/196 |
| Improper Neutralization of Special | 02-10-2019 | 9 | An issue was discovered in JetBrains TeamCity 2018.2.4. A TeamCity Project | https://blog.jetbrains.com/blog/ | A-JET-TEAM-221019/197 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Elements used in an OS Command ('OS Command Injection') | | | administrator could execute any command on the server machine. The issue was fixed in TeamCity 2018.2.5 and 2019.1.<br>**CVE ID : CVE-2019-15036** | 2019/09/26/jetbrains-security-bulletin-q2-2019/ | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 02-10-2019 | 4.3 | An issue was discovered in JetBrains TeamCity 2018.2.4. It had several XSS vulnerabilities on the settings pages. The issues were fixed in TeamCity 2019.1.<br>**CVE ID : CVE-2019-15037** | https://blog.jetbrains.com/blog/2019/09/26/jetbrains-security-bulletin-q2-2019/ | A-JET-TEAM-221019/198 |
| Improper Input Validation | 01-10-2019 | 5 | An issue was discovered in JetBrains TeamCity 2018.2.4. The TeamCity server was not using some security-related HTTP headers. The issue was fixed in TeamCity 2019.1.<br>**CVE ID : CVE-2019-15038** | N/A | A-JET-TEAM-221019/199 |
| Improper Input Validation | 01-10-2019 | 6.8 | An issue was discovered in JetBrains TeamCity 2018.2.4. It had a possible remote code execution issue. This was fixed in TeamCity 2018.2.5 and 2019.1.<br>**CVE ID : CVE-2019-15039** | https://blog.jetbrains.com/blog/2019/09/26/jetbrains-security-bulletin-q2-2019/ | A-JET-TEAM-221019/200 |
| Improper Certificate Validation | 01-10-2019 | 5 | An issue was discovered in JetBrains TeamCity 2018.2.4. It had no SSL certificate validation for some external https connections. This was fixed in TeamCity 2019.1.<br>**CVE ID : CVE-2019-15042** | N/A | A-JET-TEAM-221019/201 |
| **resharper** | | | | | |
| Untrusted | 02-10-2019 | 4.4 | JetBrains ReSharper installers | N/A | A-JET-RESH- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Search Path | | | for versions before 2019.2 had a DLL Hijacking vulnerability.<br>**CVE ID : CVE-2019-16407** | | 221019/202 |
| **ktor** | | | | | |
| Improper Input Validation | 02-10-2019 | 7.5 | JetBrains Ktor framework before 1.2.0-rc does not sanitize the username provided by the user for the LDAP protocol, leading to command injection.<br>**CVE ID : CVE-2019-12736** | https://blog.jetbrains.com/blog/2019/09/26/jetbrains-security-bulletin-q2-2019/ | A-JET-KTOR-221019/203 |
| Use of Password Hash With Insufficient Computational Effort | 02-10-2019 | 5 | UserHashedTableAuth in JetBrains Ktor framework before 1.2.0-rc uses a One-Way Hash with a Predictable Salt for storing user credentials.<br>**CVE ID : CVE-2019-12737** | https://blog.jetbrains.com/blog/2019/09/26/jetbrains-security-bulletin-q2-2019/ | A-JET-KTOR-221019/204 |
| **vim** | | | | | |
| Insecure Storage of Sensitive Information | 01-10-2019 | 5 | The JetBrains Vim plugin before version 0.52 was storing individual project data in the global vim_settings.xml file. This xml file could be synchronized to a publicly accessible GitHub repository.<br>**CVE ID : CVE-2019-14957** | https://blog.jetbrains.com/blog/2019/09/26/jetbrains-security-bulletin-q2-2019/ | A-JET-VIM-221019/205 |
| **pycharm** | | | | | |
| Uncontrolled Resource Consumption | 02-10-2019 | 5 | JetBrains PyCharm before 2019.2 was allocating a buffer of unknown size for one of the connection processes. In a very specific situation, it could lead to a remote invocation of an OOM error message because of Uncontrolled | https://blog.jetbrains.com/blog/2019/09/26/jetbrains-security-bulletin-q2-2019/ | A-JET-PYCH-221019/206 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Memory Allocation.<br>**CVE ID : CVE-2019-14958** | | |
| **toolbox** | | | | | |
| Missing Encryption of Sensitive Data | 02-10-2019 | 4.3 | JetBrains Toolbox before 1.15.5605 was resolving an internal URL via a cleartext http connection.<br>**CVE ID : CVE-2019-14959** | https://blog.jetbrains.com/blog/2019/09/26/jetbrains-security-bulletin-q2-2019/ | A-JET-TOOL-221019/207 |
| **rider** | | | | | |
| Untrusted Search Path | 01-10-2019 | 4.6 | JetBrains Rider before 2019.1.2 was using an unsigned JetBrains.Rider.Unity.Editor.Plugin.Repacked.dll file.<br>**CVE ID : CVE-2019-14960** | N/A | A-JET-RIDE-221019/208 |
| **hub** | | | | | |
| Weak Password Recovery Mechanism for Forgotten Password | 01-10-2019 | 5 | In JetBrains Hub versions earlier than 2018.4.11436, there was no option to force a user to change the password and no password expiration policy was implemented.<br>**CVE ID : CVE-2019-14955** | N/A | A-JET-HUB-221019/209 |
| **youtrack** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 01-10-2019 | 4.3 | JetBrains YouTrack versions before 2019.1.52584 had a possible XSS in the issue titles.<br>**CVE ID : CVE-2019-14952** | https://blog.jetbrains.com/blog/2019/09/26/jetbrains-security-bulletin-q2-2019/ | A-JET-YOUT-221019/210 |
| Improper Neutralizatio | 01-10-2019 | 4.3 | JetBrains YouTrack versions before 2019.2.53938 had a | N/A | A-JET-YOUT-221019/211 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| n of Input During Web Page Generation ('Cross-site Scripting') | | | possible XSS through issue attachments when using the Firefox browser.<br>**CVE ID : CVE-2019-14953** | | |
| Improper Preservation of Permissions | 02-10-2019 | 4 | JetBrains YouTrack before 2019.2.53938 was using incorrect settings, allowing a user without necessary permissions to get other project names.<br>**CVE ID : CVE-2019-14956** | https://blog.jetbrains.com/blog/2019/09/26/jetbrains-security-bulletin-q2-2019/ | A-JET-YOUT-221019/212 |
| Cross-Site Request Forgery (CSRF) | 02-10-2019 | 6.8 | JetBrains YouTrack versions before 2019.1 had a CSRF vulnerability on the settings page.<br>**CVE ID : CVE-2019-15040** | N/A | A-JET-YOUT-221019/213 |
| URL Redirection to Untrusted Site ('Open Redirect') | 01-10-2019 | 5.8 | JetBrains YouTrack versions before 2019.1.52545 allowed unbounded URL whitelisting because of Inclusion of Functionality from an Untrusted Control Sphere.<br>**CVE ID : CVE-2019-15041** | N/A | A-JET-YOUT-221019/214 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 02-10-2019 | 4.3 | In JetBrains YouTrack through 2019.2.56594, stored XSS was found on the issue page.<br>**CVE ID : CVE-2019-16171** | N/A | A-JET-YOUT-221019/215 |
| **jnoj** | | | | | |
| **jiangnan_online_judge** | | | | | |
| Improper Neutralizatio | 10-10-2019 | 4.3 | Jiangnan Online Judge (aka jnoj) 0.8.0 has XSS via the | N/A | A-JNO-JIAN-221019/216 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| n of Input During Web Page Generation ('Cross-site Scripting') | | | Problem[title] parameter to web/polygon/problem/create or web/polygon/problem/update or web/admin/problem/create. **CVE ID : CVE-2019-17489** | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 10-10-2019 | 4.3 | Jiangnan Online Judge (aka jnoj) 0.8.0 has XSS via the Problem[description] parameter to web/admin/problem/create or web/polygon/problem/update. **CVE ID : CVE-2019-17491** | N/A | A-JNO-JIAN-221019/217 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 10-10-2019 | 4.3 | Jiangnan Online Judge (aka jnoj) 0.8.0 has XSS via the Problem[sample_input] parameter to web/admin/problem/create or web/polygon/problem/update. **CVE ID : CVE-2019-17493** | N/A | A-JNO-JIAN-221019/218 |
| **joomlashack** | | | | | |
| **shack_forms_pro** | | | | | |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 09-10-2019 | 7.5 | The Shack Forms Pro extension before 4.0.32 for Joomla! allows path traversal via a file attachment. **CVE ID : CVE-2019-17399** | N/A | A-JOO-SHAC-221019/219 |
| **joyplus-cms_project** | | | | | |
| **joyplus-cms** | | | | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 04-10-2019 | 5 | joyplus-cms 1.6.0 allows manager/admin_pic.php?rootpath= absolute path traversal. **CVE ID : CVE-2019-17175** | N/A | A-JOY-JOYP-221019/220 |
| **Kmplayer** | | | | | |
| **kmplayer** | | | | | |
| Out-of-bounds Write | 08-10-2019 | 4.6 | KMPlayer 4.2.2.31 allows a User Mode Write AV starting at utils!src_new+0x000000000014d6ee. **CVE ID : CVE-2019-17259** | N/A | A-KMP-KMPL-221019/221 |
| **koji_project** | | | | | |
| **koji** | | | | | |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 09-10-2019 | 4 | Koji through 1.18.0 allows remote Directory Traversal, with resultant Privilege Escalation. **CVE ID : CVE-2019-17109** | https://docs.pagure.org/koji/CVE-2019-17109/, https://pagure.io/koji/commits/master | A-KOJ-KOJI-221019/222 |
| **kslabs** | | | | | |
| **ksweb** | | | | | |
| Improper Control of Generation of Code ('Code Injection') | 03-10-2019 | 6.5 | The KSLABS KSWEB (aka ru.kslabs.ksweb) application 3.93 for Android allows authenticated remote code execution via a POST request to the AJAX handler with the configFile parameter set to the arbitrary file to be written to (and the config_text parameter | N/A | A-KSL-KSWE-221019/223 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | set to the content of the file to be created). This can be a PHP file that is written to in the public web directory and subsequently executed. The attacker must have network connectivity to the PHP server that is running on the Android device.<br>**CVE ID : CVE-2019-15766** | | |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 03-10-2019 | 4 | KSLabs KSWEB 3.93 allows ../ directory traversal, as demonstrated by the hostFile parameter.<br>**CVE ID : CVE-2019-16198** | N/A | A-KSL-KSWE-221019/224 |
| **Kubernetes** | | | | | |
| **kube-state-metrics** | | | | | |
| Information Exposure | 03-10-2019 | 5 | A security issue was discovered in kube-state-metrics 1.7.x before 1.7.2. An experimental feature was added to v1.7.0 and v1.7.1 that enabled annotations to be exposed as metrics. By default, kube-state-metrics metrics only expose metadata about Secrets. However, a combination of the default kubectl behavior and this new feature can cause the entire secret content to end up in metric labels, thus inadvertently exposing the secret content in metrics.<br>**CVE ID : CVE-2019-17110** | N/A | A-KUB-KUBE-221019/225 |
| **laravel-admin** | | | | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **laravel-admin** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 10-10-2019 | 3.5 | z-song laravel-admin 1.7.3 has XSS via the Slug or Name on the Roles screen, because of mishandling on the "Operation log" screen. **CVE ID : CVE-2019-17433** | N/A | A-LAR-LARA-221019/226 |
| **lavalite** | | | | | |
| **lavalite** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 10-10-2019 | 3.5 | LavaLite through 5.7 has XSS via a crafted account name that is mishandled on the Manage Clients screen. **CVE ID : CVE-2019-17434** | N/A | A-LAV-LAVA-221019/227 |
| **libfwsi_project** | | | | | |
| **libfwsi** | | | | | |
| Out-of-bounds Read | 06-10-2019 | 2.1 | ** DISPUTED ** In libyal libfwsi before 20191006, libfwsi_extension_block_copy_from_byte_stream in libfwsi_extension_block.c has a heap-based buffer over-read because rejection of an unsupported size only considers values less than 6, even though values of 6 and 7 are also unsupported. NOTE: the vendor has disputed this as described in the GitHub issue. **CVE ID : CVE-2019-17263** | N/A | A-LIB-LIBF-221019/228 |
| **liblnk_project** | | | | | |
| **liblnk** | | | | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Out-of-bounds Read | 06-10-2019 | 6.8 | ** DISPUTED ** In libyal liblnk before 20191006, liblnk_location_information_read_data in liblnk_location_information.c has a heap-based buffer over-read because an incorrect variable name is used for a certain offset. NOTE: the vendor has disputed this as described in the GitHub issue. **CVE ID : CVE-2019-17264** | N/A | A-LIB-LIBL-221019/229 |
| Out-of-bounds Read | 09-10-2019 | 2.1 | ** DISPUTED ** libyal liblnk 20191006 has a heap-based buffer over-read in the network_share_name_offset>20 code block of liblnk_location_information_read_data in liblnk_location_information.c, a different issue than CVE-2019-17264. NOTE: the vendor has disputed this as described in the GitHub issue. **CVE ID : CVE-2019-17401** | N/A | A-LIB-LIBL-221019/230 |
| **libpl_droidsonroids_gif_project** | | | | | |
| **libpl_droidsonroids_gif** | | | | | |
| Double Free | 03-10-2019 | 7.5 | A double free vulnerability in the DDGifSlurp function in decoding.c in libpl_droidsonroids_gif before 1.2.15, as used in WhatsApp for Android before 2.19.244, allows remote attackers to execute arbitrary code or cause a denial of service. **CVE ID : CVE-2019-11932** | https://www.facebook.com/security/advisories/cve-2019-11932 | A-LIB-LIBP-221019/231 |
| **Libpng** | | | | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **libpng** | | | | | |
| Missing Release of Resource after Effective Lifetime | 09-10-2019 | 4.3 | libpng 1.6.37 has memory leaks in png_malloc_warn and png_create_info_struct. **CVE ID : CVE-2019-17371** | N/A | A-LIB-LIBP-221019/232 |
| **Liferay** | | | | | |
| **liferay_portal** | | | | | |
| Deserialization of Untrusted Data | 04-10-2019 | 6.5 | Liferay Portal CE 6.2.5 allows remote command execution because of deserialization of a JSON payload. **CVE ID : CVE-2019-16891** | N/A | A-LIF-LIFE-221019/233 |
| **Linuxmint** | | | | | |
| **mintinstall** | | | | | |
| Deserialization of Untrusted Data | 02-10-2019 | 6.8 | mintinstall (aka Software Manager) 7.9.9 for Linux Mint allows code execution if a REVIEWS_CACHE file is controlled by an attacker, because an unpickle occurs. This is resolved in 8.0.0 and backports. **CVE ID : CVE-2019-17080** | N/A | A-LIN-MINT-221019/234 |
| **lodev** | | | | | |
| **lodepngl** | | | | | |
| Missing Release of Resource after Effective Lifetime | 04-10-2019 | 5 | HuffmanTree_makeFromFrequencies in lodepng.c in LodePNG through 2019-09-28, as used in WinPR in FreeRDP and other products, has a memory leak because a supplied realloc pointer (i.e., the first argument to realloc) is also used for a realloc return value. | N/A | A-LOD-LODE-221019/235 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2019-17178** | | |
| **lqd** | | | | | |
| **liquid_speech_balloon** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 10-10-2019 | 4.3 | The liquid-speech-balloon (aka LIQUID SPEECH BALLOON) plugin 1.0.5 for WordPress allows XSS with Internet Explorer.<br>**CVE ID : CVE-2019-17070** | N/A | A-LQD-LIQU-221019/236 |
| **Matrixssl** | | | | | |
| **matrixssl** | | | | | |
| Use of a Broken or Risky Cryptographic Algorithm | 03-10-2019 | 4.3 | MatrixSSL 4.2.1 and earlier contains a timing side channel in ECDSA signature generation. This allows a local or a remote attacker, able to measure the duration of hundreds to thousands of signing operations, to compute the private key used. The issue occurs because crypto/pubkey/ecc_math.c scalar multiplication leaks the bit length of the scalar.<br>**CVE ID : CVE-2019-13629** | N/A | A-MAT-MATR-221019/237 |
| **Metinfo** | | | | | |
| **metinfo** | | | | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 10-10-2019 | 6.5 | An issue was discovered in MetInfo 7.0. There is SQL injection via the admin/?n=language&c=language_general&a=doSearchParameter appno parameter, a different issue than CVE-2019-16997. | N/A | A-MET-METI-221019/238 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2019-17418** | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 10-10-2019 | 6.5 | An issue was discovered in MetInfo 7.0. There is SQL injection via the admin/?n=user&c=admin_user&a=doGetUserInfo id parameter.<br>**CVE ID : CVE-2019-17419** | N/A | A-MET-METI-221019/239 |
| **Microfocus** | | | | | |
| **enterprise_developer** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 02-10-2019 | 4.3 | Reflected XSS on Micro Focus Enterprise Developer and Enterprise Server, all versions prior to version 3.0 Patch Update 20, version 4.0 Patch Update 12, and version 5.0 Patch Update 2. The vulnerability could be exploited to redirect a user to a malicious page or forge certain types of web requests.<br>**CVE ID : CVE-2019-11651** | N/A | A-MIC-ENTE-221019/240 |
| **enterprise_server** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 02-10-2019 | 4.3 | Reflected XSS on Micro Focus Enterprise Developer and Enterprise Server, all versions prior to version 3.0 Patch Update 20, version 4.0 Patch Update 12, and version 5.0 Patch Update 2. The vulnerability could be exploited to redirect a user to a malicious page or forge certain types of web requests.<br>**CVE ID : CVE-2019-11651** | N/A | A-MIC-ENTE-221019/241 |
| **Microsoft** | | | | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **excel_services** | | | | | |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 10-10-2019 | 9.3 | A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory, aka 'Microsoft Excel Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1327.<br>**CVE ID : CVE-2019-1331** | N/A | A-MIC-EXCE-221019/242 |
| **sql_server_management_studio** | | | | | |
| Incorrect Permission Assignment for Critical Resource | 10-10-2019 | 4 | An information disclosure vulnerability exists in Microsoft SQL Server Management Studio (SSMS) when it improperly enforces permissions, aka 'SQL Server Management Studio Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1376.<br>**CVE ID : CVE-2019-1313** | N/A | A-MIC-SQL_-221019/243 |
| Incorrect Permission Assignment for Critical Resource | 10-10-2019 | 4 | An information disclosure vulnerability exists in Microsoft SQL Server Management Studio (SSMS) when it improperly enforces permissions, aka 'SQL Server Management Studio Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1313.<br>**CVE ID : CVE-2019-1376** | N/A | A-MIC-SQL_-221019/244 |
| **chakracore** | | | | | |
| Improper Restriction of | 10-10-2019 | 7.6 | A remote code execution vulnerability exists in the way that the Chakra scripting | N/A | A-MIC-CHAK-221019/245 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Operations within the Bounds of a Memory Buffer | | | engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1308, CVE-2019-1335, CVE-2019-1366.<br>**CVE ID : CVE-2019-1307** | | |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 10-10-2019 | 7.6 | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1307, CVE-2019-1335, CVE-2019-1366.<br>**CVE ID : CVE-2019-1308** | N/A | A-MIC-CHAK-221019/246 |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 10-10-2019 | 7.6 | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1307, CVE-2019-1308, CVE-2019-1366.<br>**CVE ID : CVE-2019-1335** | N/A | A-MIC-CHAK-221019/247 |
| Improper Restriction of Operations within the Bounds of a | 10-10-2019 | 7.6 | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine | N/A | A-MIC-CHAK-221019/248 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Memory Buffer | | | Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1307, CVE-2019-1308, CVE-2019-1335.<br>**CVE ID : CVE-2019-1366** | | |
| **edge** | | | | | |
| Authentication Bypass by Spoofing | 10-10-2019 | 4.3 | A spoofing vulnerability exists when Microsoft Browsers does not properly parse HTTP content, aka 'Microsoft Browser Spoofing Vulnerability'. This CVE ID is unique from CVE-2019-1357.<br>**CVE ID : CVE-2019-0608** | N/A | A-MIC-EDGE-221019/249 |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 10-10-2019 | 7.6 | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1308, CVE-2019-1335, CVE-2019-1366.<br>**CVE ID : CVE-2019-1307** | N/A | A-MIC-EDGE-221019/250 |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 10-10-2019 | 7.6 | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1307, CVE-2019-1335, CVE-2019-1366. | N/A | A-MIC-EDGE-221019/251 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2019-1308** | | |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 10-10-2019 | 7.6 | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1307, CVE-2019-1308, CVE-2019-1366.<br>**CVE ID : CVE-2019-1335** | N/A | A-MIC-EDGE-221019/252 |
| Authentication Bypass by Spoofing | 10-10-2019 | 4.3 | A spoofing vulnerability exists when Microsoft Browsers improperly handle browser cookies, aka 'Microsoft Browser Spoofing Vulnerability'. This CVE ID is unique from CVE-2019-0608.<br>**CVE ID : CVE-2019-1357** | N/A | A-MIC-EDGE-221019/253 |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 10-10-2019 | 7.6 | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1307, CVE-2019-1308, CVE-2019-1335.<br>**CVE ID : CVE-2019-1366** | N/A | A-MIC-EDGE-221019/254 |
| **office** | | | | | |
| Improper Restriction of Operations within the | 10-10-2019 | 9.3 | A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory, aka | N/A | A-MIC-OFFI-221019/255 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Bounds of a Memory Buffer | | | 'Microsoft Excel Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1327.<br>**CVE ID : CVE-2019-1331** | | |
| **office_365_proplus** | | | | | |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 10-10-2019 | 9.3 | A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory, aka 'Microsoft Excel Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1331.<br>**CVE ID : CVE-2019-1327** | N/A | A-MIC-OFFI-221019/256 |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 10-10-2019 | 9.3 | A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory, aka 'Microsoft Excel Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1327.<br>**CVE ID : CVE-2019-1331** | N/A | A-MIC-OFFI-221019/257 |
| **internet_explorer** | | | | | |
| Authentication Bypass by Spoofing | 10-10-2019 | 4.3 | A spoofing vulnerability exists when Microsoft Browsers does not properly parse HTTP content, aka 'Microsoft Browser Spoofing Vulnerability'. This CVE ID is unique from CVE-2019-1357.<br>**CVE ID : CVE-2019-0608** | N/A | A-MIC-INTE-221019/258 |
| Improper Restriction of | 10-10-2019 | 7.1 | A remote code execution vulnerability exists in the way that the VBScript engine | N/A | A-MIC-INTE-221019/259 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Operations within the Bounds of a Memory Buffer | | | handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1239.<br>**CVE ID : CVE-2019-1238** | | |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 10-10-2019 | 7.6 | A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1238.<br>**CVE ID : CVE-2019-1239** | N/A | A-MIC-INTE-221019/260 |
| Authentication Bypass by Spoofing | 10-10-2019 | 4.3 | A spoofing vulnerability exists when Microsoft Browsers improperly handle browser cookies, aka 'Microsoft Browser Spoofing Vulnerability'. This CVE ID is unique from CVE-2019-0608.<br>**CVE ID : CVE-2019-1357** | N/A | A-MIC-INTE-221019/261 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 10-10-2019 | 4.3 | The liquid-speech-balloon (aka LIQUID SPEECH BALLOON) plugin 1.0.5 for WordPress allows XSS with Internet Explorer.<br>**CVE ID : CVE-2019-17070** | N/A | A-MIC-INTE-221019/262 |
| **sharepoint_server** | | | | | |
| Improper Restriction of Operations within the Bounds of a Memory | 10-10-2019 | 9.3 | A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory, aka 'Microsoft Excel Remote Code Execution Vulnerability'. This | N/A | A-MIC-SHAR-221019/263 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Buffer | | | CVE ID is unique from CVE-2019-1327.<br>**CVE ID : CVE-2019-1331** | | |
| **sharepoint_enterprise_server** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 10-10-2019 | 3.5 | A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'.<br>**CVE ID : CVE-2019-1070** | N/A | A-MIC-SHAR-221019/264 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 10-10-2019 | 3.5 | A spoofing vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft SharePoint Spoofing Vulnerability'.<br>**CVE ID : CVE-2019-1328** | N/A | A-MIC-SHAR-221019/265 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 10-10-2019 | 3.5 | An elevation of privilege vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft SharePoint Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1330.<br>**CVE ID : CVE-2019-1329** | N/A | A-MIC-SHAR-221019/266 |
| Improper Privilege Management | 10-10-2019 | 4 | An elevation of privilege vulnerability exists in Microsoft SharePoint, aka 'Microsoft SharePoint | N/A | A-MIC-SHAR-221019/267 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1329.<br>**CVE ID : CVE-2019-1330** | | |
| **office_online_server** | | | | | |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 10-10-2019 | 9.3 | A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory, aka 'Microsoft Excel Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1327.<br>**CVE ID : CVE-2019-1331** | N/A | A-MIC-OFFI-221019/268 |
| **sharepoint_foundation** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 10-10-2019 | 3.5 | A spoofing vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft SharePoint Spoofing Vulnerability'.<br>**CVE ID : CVE-2019-1328** | N/A | A-MIC-SHAR-221019/269 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 10-10-2019 | 3.5 | An elevation of privilege vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft SharePoint Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1330.<br>**CVE ID : CVE-2019-1329** | N/A | A-MIC-SHAR-221019/270 |
| Improper | 10-10-2019 | 4 | An elevation of privilege | N/A | A-MIC- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Privilege Management | | | vulnerability exists in Microsoft SharePoint, aka 'Microsoft SharePoint Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1329.<br>**CVE ID : CVE-2019-1330** | | SHAR-221019/271 |
| **excel** | | | | | |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 10-10-2019 | 9.3 | A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory, aka 'Microsoft Excel Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1331.<br>**CVE ID : CVE-2019-1327** | N/A | A-MIC-EXCE-221019/272 |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 10-10-2019 | 9.3 | A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory, aka 'Microsoft Excel Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1327.<br>**CVE ID : CVE-2019-1331** | N/A | A-MIC-EXCE-221019/273 |
| **open_enclave_software_development_kit** | | | | | |
| Information Exposure | 10-10-2019 | 5 | An information disclosure vulnerability exists when affected Open Enclave SDK versions improperly handle objects in memory, aka 'Open Enclave SDK Information Disclosure Vulnerability'.<br>**CVE ID : CVE-2019-1369** | N/A | A-MIC-OPEN-221019/274 |
| **Mozilla** | | | | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **firefox** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 01-10-2019 | 4.3 | JetBrains YouTrack versions before 2019.2.53938 had a possible XSS through issue attachments when using the Firefox browser.<br>**CVE ID : CVE-2019-14953** | N/A | A-MOZ-FIRE-221019/275 |
| **mpc-hc** | | | | | |
| **mpc-hc** | | | | | |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 08-10-2019 | 4.6 | MPC-HC through 1.7.13 allows a Read Access Violation on a Block Data Move starting at mpc_hc!memcpy+0x000000000000004e.<br>**CVE ID : CVE-2019-17260** | N/A | A-MPC-MPC--221019/276 |
| **netreo** | | | | | |
| **omnicenter** | | | | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 09-10-2019 | 5 | Netreo OmniCenter through 12.1.1 allows unauthenticated SQL Injection (Boolean Based Blind) in the redirect parameters and parameter name of the login page through a GET request. The injection allows an attacker to read sensitive information from the database used by the application.<br>**CVE ID : CVE-2019-17128** | N/A | A-NET-OMNI-221019/277 |
| **Nlnetlabs** | | | | | |
| **unbound** | | | | | |
| Improper Restriction of | 03-10-2019 | 5 | Unbound before 1.9.4 accesses uninitialized memory, which allows remote attackers to | N/A | A-NLN-UNBO- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Operations within the Bounds of a Memory Buffer | | | trigger a crash via a crafted NOTIFY query. The source IP address of the query must match an access-control rule.<br>**CVE ID : CVE-2019-16866** | | 221019/278 |
| **online_store_system_project** | | | | | |
| **online_store_system** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 01-10-2019 | 3.5 | Vulnerability in Online Store v1.0, Stored XSS in user_view.php where adidas_member_user variable is not sanitized.<br>**CVE ID : CVE-2019-8288** | N/A | A-ONL-ONLI-221019/279 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 01-10-2019 | 3.5 | Vulnerability in Online Store v1.0, stored XSS in admin/user_view.php adidas_member_email variable<br>**CVE ID : CVE-2019-8289** | N/A | A-ONL-ONLI-221019/280 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 01-10-2019 | 4.3 | Vulnerability in Online Store v1.0, The registration form requirements for the member email format can be bypassed by posting directly to sent_register.php allowing special characters to be included and an XSS payload to be injected.<br>**CVE ID : CVE-2019-8290** | N/A | A-ONL-ONLI-221019/281 |
| Improper Limitation of a Pathname to a Restricted Directory | 01-10-2019 | 6.4 | Online Store System v1.0 delete_file.php doesn't check to see if a user has administrative rights nor does it check for path traversal. | N/A | A-ONL-ONLI-221019/282 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ('Path Traversal') | | | **CVE ID : CVE-2019-8291** | | |
| Missing Authentication for Critical Function | 01-10-2019 | 6.4 | Online Store System v1.0 delete_product.php doesn't check to see if a user authtenticated or has administrative rights allowing arbitrary product deletion.<br>**CVE ID : CVE-2019-8292** | N/A | A-ONL-ONLI-221019/283 |
| **Open-emr** | | | | | |
| **openemr** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 04-10-2019 | 4.3 | XSS in library/custom_template/add_template.php in OpenEMR through 5.0.2 allows a malicious user to execute code in the context of a victim's browser via a crafted list_id query parameter.<br>**CVE ID : CVE-2019-17179** | N/A | A-OPE-OPEN-221019/284 |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 05-10-2019 | 7.5 | OpenEMR through 5.0.2 has SQL Injection in the Lifestyle demographic filter criteria in library/clinical_rules.php that affects library/patient.inc.<br>**CVE ID : CVE-2019-17197** | N/A | A-OPE-OPEN-221019/285 |
| **openmpt** | | | | | |
| **libopenmpt** | | | | | |
| Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') | 04-10-2019 | 7.5 | In libopenmpt before 0.3.19 and 0.4.x before 0.4.9, ModPlug_InstrumentName and ModPlug_SampleName in libopenmpt_modplug.c do not restrict the lengths of libmodplug output-buffer | N/A | A-OPE-LIBO-221019/286 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | strings in the C API, leading to a buffer overflow.<br>**CVE ID : CVE-2019-17113** | | |
| **openproject** | | | | | |
| **openproject** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 09-10-2019 | 4.3 | An XSS vulnerability in project list in OpenProject before 9.0.4 and 10.x before 10.0.2 allows remote attackers to inject arbitrary web script or HTML via the sortBy parameter because error messages are mishandled.<br>**CVE ID : CVE-2019-17092** | https://www.openproject.org/release-notes/openproject-10-0-2/, https://www.openproject.org/release-notes/openproject-9-0-4/ | A-OPE-OPEN-221019/287 |
| **otcms** | | | | | |
| **otcms** | | | | | |
| Improper Input Validation | 09-10-2019 | 6.5 | OTCMS v3.85 allows arbitrary PHP Code Execution because admin/sysCheckFile_deal.php blocks "into outfile" in a SELECT statement, but does not block the "into/**/outfile" manipulation. Therefore, the attacker can create a .php file.<br>**CVE ID : CVE-2019-17370** | N/A | A-OTC-OTCM-221019/288 |
| **Pbootcms** | | | | | |
| **Pbootcms** | | | | | |
| Improper Neutralization of Input During Web Page Generation | 10-10-2019 | 3.5 | PbootCMS 2.0.2 allows XSS via vectors involving the Pboot/admin.php?p=/Single/index/mcode/1 and Pboot/?contact/ URIs. | N/A | A-PBO-PBOO-221019/289 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ('Cross-site Scripting') | | | **CVE ID : CVE-2019-17417** | | |
| **pcprotect** | | | | | |
| **antivirus** | | | | | |
| Improper Privilege Management | 07-10-2019 | 7.2 | PC Protect Antivirus v4.14.31 installs by default to %PROGRAMFILES(X86)%\PC Protect with very weak folder permissions, granting any user full permission "Everyone: (F)" to the contents of the directory and its subfolders. In addition, the program installs a service called SecurityService that runs as LocalSystem. This allows any user to escalate privileges to "NT AUTHORITY\SYSTEM" by substituting the service's binary with a Trojan horse. **CVE ID : CVE-2019-16913** | N/A | A-PCP-ANTI-221019/290 |
| **pi-hole** | | | | | |
| **pi-hole** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 09-10-2019 | 6.8 | Pi-Hole 4.3 allows Command Injection. **CVE ID : CVE-2019-13051** | N/A | A-PI--PI-H-221019/291 |
| **Pivotal** | | | | | |
| **apps_manager** | | | | | |
| Incorrect Permission Assignment for Critical | 01-10-2019 | 4 | Pivotal Application Manager, versions 666.0.x prior to 666.0.36, versions 667.0.x prior to 667.0.22, versions | https://pivotal.io/security/cve-2019- | A-PIV-APPS-221019/292 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Resource | | | 668.0.x prior to 668.0.21, versions 669.0.x prior to 669.0.13, and versions 670.0.x prior to 670.0.7, contain a vulnerability where a remote authenticated user can create an app with a name such that a csv program can interpret into a formula and gets executed. The malicious user can possibly gain access to a usage report that requires a higher privilege.<br>**CVE ID : CVE-2019-11275** | 11275 | |
| **pivotal_software** | | | | | |
| **pivotal_application_service** | | | | | |
| Incorrect Permission Assignment for Critical Resource | 01-10-2019 | 4 | Pivotal Application Manager, versions 666.0.x prior to 666.0.36, versions 667.0.x prior to 667.0.22, versions 668.0.x prior to 668.0.21, versions 669.0.x prior to 669.0.13, and versions 670.0.x prior to 670.0.7, contain a vulnerability where a remote authenticated user can create an app with a name such that a csv program can interpret into a formula and gets executed. The malicious user can possibly gain access to a usage report that requires a higher privilege.<br>**CVE ID : CVE-2019-11275** | https://pivotal.io/security/cve-2019-11275 | A-PIV-PIVO-221019/293 |
| **Putty** | | | | | |
| **putty** | | | | | |
| Allocation of Resources Without | 01-10-2019 | 7.5 | PuTTY before 0.73 on Windows improperly opens port-forwarding listening | N/A | A-PUT-PUTT- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Limits or Throttling | | | sockets, which allows attackers to listen on the same port to steal an incoming connection.<br>**CVE ID : CVE-2019-17067** | | 221019/294 |
| Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') | 01-10-2019 | 5 | PuTTY before 0.73 mishandles the "bracketed paste mode" protection mechanism, which may allow a session to be affected by malicious clipboard content.<br>**CVE ID : CVE-2019-17068** | N/A | A-PUT-PUTT-221019/295 |
| Improper Input Validation | 01-10-2019 | 5 | PuTTY before 0.73 might allow remote SSH-1 servers to cause a denial of service by accessing freed memory locations via an SSH1_MSG_DISCONNECT message.<br>**CVE ID : CVE-2019-17069** | N/A | A-PUT-PUTT-221019/296 |
| **Python** | | | | | |
| **pillow** | | | | | |
| Allocation of Resources Without Limits or Throttling | 04-10-2019 | 4.3 | An issue was discovered in Pillow before 6.2.0. When reading specially crafted invalid image files, the library can either allocate very large amounts of memory or take an extremely long period of time to process the image.<br>**CVE ID : CVE-2019-16865** | N/A | A-PYT-PILL-221019/297 |
| **realbigplugins** | | | | | |
| **client_dash** | | | | | |
| Improper Neutralization of Input During Web | 10-10-2019 | 4.3 | The client-dash (aka Client Dash) plugin 2.1.4 for WordPress allows XSS. | N/A | A-REA-CLIE-221019/298 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Page Generation ('Cross-site Scripting') | | | **CVE ID : CVE-2019-17071** | | |
| **Redhat** | | | | | |
| **jboss_operations_network** | | | | | |
| Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection') | 03-10-2019 | 6.8 | It was found that the fix for CVE-2014-0114 had been reverted in JBoss Operations Network 3 (JON). This flaw allows attackers to manipulate ClassLoader properties on a vulnerable server. Exploits that have been published rely on ClassLoader properties that are exposed such as those in JON 3. Additional information can be found in the Red Hat Knowledgebase article: https://access.redhat.com/site/solutions/869353. Note that while multiple products released patches for the original CVE-2014-0114 flaw, the reversion described by this CVE-2019-3834 flaw only occurred in JON 3.<br>**CVE ID : CVE-2019-3834** | https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-3834 | A-RED-JBOS-221019/299 |
| **jboss_enterprise_application_platform** | | | | | |
| Deserialization of Untrusted Data | 01-10-2019 | 7.5 | A series of deserialization vulnerabilities have been discovered in Codehaus 1.9.x implemented in EAP 7. This CVE fixes CVE-2017-17485, CVE-2017-7525, CVE-2017-15095, CVE-2018-5968, CVE-2018-7489, CVE-2018-1000873, CVE-2019-12086 reported for FasterXML | https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-10202 | A-RED-JBOS-221019/300 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | jackson-databind by implementing a whitelist approach that will mitigate these vulnerabilities and future ones alike.<br>**CVE ID : CVE-2019-10202** | | |
| **single_sign-on** | | | | | |
| Information Exposure Through Log Files | 02-10-2019 | 4.3 | A flaw was found in, all under 2.0.20, in the Undertow DEBUG log for io.undertow.request.security. If enabled, an attacker could abuse this flaw to obtain the user's credentials from the log files.<br>**CVE ID : CVE-2019-10212** | https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-10212 | A-RED-SING-221019/301 |
| **undertow** | | | | | |
| Information Exposure Through Log Files | 02-10-2019 | 4.3 | A flaw was found in, all under 2.0.20, in the Undertow DEBUG log for io.undertow.request.security. If enabled, an attacker could abuse this flaw to obtain the user's credentials from the log files.<br>**CVE ID : CVE-2019-10212** | https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-10212 | A-RED-UNDE-221019/302 |
| **jboss_data_grid** | | | | | |
| Information Exposure Through Log Files | 02-10-2019 | 4.3 | A flaw was found in, all under 2.0.20, in the Undertow DEBUG log for io.undertow.request.security. If enabled, an attacker could abuse this flaw to obtain the user's credentials from the log files.<br>**CVE ID : CVE-2019-10212** | https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-10212 | A-RED-JBOS-221019/303 |
| **jboss_fuse** | | | | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Information Exposure Through Log Files | 02-10-2019 | 4.3 | A flaw was found in, all under 2.0.20, in the Undertow DEBUG log for io.undertow.request.security. If enabled, an attacker could abuse this flaw to obtain the user's credentials from the log files. **CVE ID : CVE-2019-10212** | https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-10212 | A-RED-JBOS-221019/304 |
| **Redmine** | | | | | |
| **redmine** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 10-10-2019 | 4.3 | In Redmine before 3.4.11 and 4.0.x before 4.0.4, persistent XSS exists due to textile formatting errors. **CVE ID : CVE-2019-17427** | N/A | A-RED-REDM-221019/305 |
| **rpyc_project** | | | | | |
| **rpyc** | | | | | |
| Missing Authorization | 03-10-2019 | 5 | In RPyC 4.1.x through 4.1.1, a remote attacker can dynamically modify object attributes to construct a remote procedure call that executes code for an RPyC service with default configuration settings. **CVE ID : CVE-2019-16328** | N/A | A-RPY-RPYC-221019/306 |
| **salesagility** | | | | | |
| **suitecrm** | | | | | |
| Server-Side Request Forgery (SSRF) | 02-10-2019 | 7.5 | SalesAgility SuiteCRM 7.10.x 7.10.19 and 7.11.x before and 7.11.7 has SSRF. **CVE ID : CVE-2019-13335** | https://docs.suitecrm.com/admin/releases/7.10.x/#_7_10_20, | A-SAL-SUIT-221019/307 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | https://docs.suitecrm.com/admin/releases/7.11.x/#_7_11_7, https://docs.suitecrm.com/admin/releases/7.11.x/#_7_11_8 | |
| Improper Privilege Management | 02-10-2019 | 7.5 | SuiteCRM 7.11.x and 7.10.x before 7.11.8 and 7.10.20 is vulnerable to vertical privilege escalation.<br>**CVE ID : CVE-2019-14454** | https://docs.suitecrm.com/admin/releases/7.10.x/#_7_10_20, https://docs.suitecrm.com/admin/releases/7.11.x/#_7_11_8 | A-SAL-SUIT-221019/308 |
| **SAP** | | | | | |
| **netweaver_process_integration** | | | | | |
| Missing Authorization | 08-10-2019 | 4 | SAP NetWeaver Process Integration (B2B Toolkit), before versions 1.0 and 2.0, does not perform necessary authorization checks for an authenticated user, allowing the import of B2B table content that leads to Missing Authorization Check.<br>**CVE ID : CVE-2019-0367** | https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=528123050 | A-SAP-NETW-221019/309 |
| **businessobjects_business_intelligence_platform** | | | | | |
| Improper Neutralizatio | 08-10-2019 | 3.5 | SAP BusinessObjects Business Intelligence Platform (Web | https://wiki.scn.sap.c | A-SAP-BUSI-221019/310 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| n of Input During Web Page Generation ('Cross-site Scripting') | | | Intelligence HTML interface), before versions 4.2 and 4.3, does not sufficiently encode user-controlled inputs and allows execution of scripts in the chart title resulting in reflected Cross-Site Scripting<br>**CVE ID : CVE-2019-0374** | om/wiki/pages/viewpage.action?pageId=528123050 | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 08-10-2019 | 3.5 | SAP BusinessObjects Business Intelligence Platform (Web Intelligence HTML interface), before versions 4.2 and 4.3, does not sufficiently encode user-controlled inputs and allows execution of scripts in the export dialog box of the report name resulting in reflected Cross-Site Scripting.<br>**CVE ID : CVE-2019-0375** | https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=528123050 | A-SAP-BUSI-221019/311 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 08-10-2019 | 3.5 | SAP BusinessObjects Business Intelligence Platform (Web Intelligence HTML interface), before versions 4.2 and 4.3, does not sufficiently encode user-controlled inputs and allows an attacker to save malicious scripts in the publication name, which can be executed later by the victim, resulting in Stored Cross-Site Scripting.<br>**CVE ID : CVE-2019-0376** | https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=528123050 | A-SAP-BUSI-221019/312 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site | 08-10-2019 | 3.5 | SAP BusinessObjects Business Intelligence Platform (Web Intelligence HTML interface), before versions 4.2, does not sufficiently encode user-controlled inputs and allows an attacker to store malicious | https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=528123050 | A-SAP-BUSI-221019/313 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Scripting') | | | scripts in the input controls, resulting in Stored Cross-Site Scripting.<br>**CVE ID : CVE-2019-0377** | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 08-10-2019 | 3.5 | SAP BusinessObjects Business Intelligence Platform (Web Intelligence HTML interface), before version 4.2, does not sufficiently encode user-controlled inputs and allows an attacker to store malicious scripts in the file name of the background image resulting in Stored Cross-Site Scripting.<br>**CVE ID : CVE-2019-0378** | https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=528123050 | A-SAP-BUSI-221019/314 |
| **financial_consolidation** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 08-10-2019 | 3.5 | SAP Financial Consolidation, before versions 10.0 and 10.1, does not sufficiently encode user-controlled inputs, which allows an attacker to execute scripts by uploading files containing malicious scripts, leading to reflected cross site scripting vulnerability.<br>**CVE ID : CVE-2019-0369** | https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=528123050 | A-SAP-FINA-221019/315 |
| XML Injection (aka Blind XPath Injection) | 08-10-2019 | 6.4 | Due to missing input validation, SAP Financial Consolidation, before versions 10.0 and 10.1, enables an attacker to use crafted input to interfere with the structure of the surrounding query leading to XPath Injection.<br>**CVE ID : CVE-2019-0370** | https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=528123050 | A-SAP-FINA-221019/316 |
| **S-cms** | | | | | |
| **S-cms** | | | | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 09-10-2019 | 4.3 | S-CMS v1.5 has XSS in tpl.php via the member/member_login.php from parameter.<br>**CVE ID : CVE-2019-17368** | N/A | A-S-C-S-CM-221019/317 |
| **signal** | | | | | |
| **signal_private_messenger** | | | | | |
| Improper Input Validation | 05-10-2019 | 7.5 | ** DISPUTED ** The WebRTC component in the Signal Private Messenger application through 4.47.7 for Android processes videoconferencing RTP packets before a callee chooses to answer a call, which might make it easier for remote attackers to cause a denial of service or possibly have unspecified other impact via malformed packets. NOTE: the vendor plans to continue this behavior for performance reasons unless a WebRTC design change occurs.<br>**CVE ID : CVE-2019-17192** | N/A | A-SIG-SIGN-221019/318 |
| **private_messenger** | | | | | |
| Improper Input Validation | 05-10-2019 | 5 | The Signal Private Messenger application before 4.47.7 for Android allows a caller to force a call to be answered, without callee user interaction, via a connect message. The existence of the call is noticeable to the callee; however, the audio channel may be open before the callee can block eavesdropping. | N/A | A-SIG-PRIV-221019/319 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2019-17191** | | |
| **sitos** | | | | | |
| **sitos_six** | | | | | |
| Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') | 07-10-2019 | 10 | SITOS six Build v6.2.1 allows an attacker to inject arbitrary PHP commands. As a result, an attacker can compromise the running server and execute system commands in the context of the web user.<br>**CVE ID : CVE-2019-15746** | N/A | A-SIT-SITO-221019/320 |
| Improper Privilege Management | 07-10-2019 | 6.5 | SITOS six Build v6.2.1 allows a user with the user role of Seminar Coordinator to escalate their permission to the Systemadministrator role due to insufficient checks on the server side.<br>**CVE ID : CVE-2019-15747** | N/A | A-SIT-SITO-221019/321 |
| Unrestricted Upload of File with Dangerous Type | 07-10-2019 | 7.5 | SITOS six Build v6.2.1 permits unauthorised users to upload and import a SCORM 2004 package by browsing directly to affected pages. An unauthenticated attacker could use the upload and import functionality to import a malicious SCORM package that includes a PHP file, which could execute arbitrary PHP code.<br>**CVE ID : CVE-2019-15748** | N/A | A-SIT-SITO-221019/322 |
| Weak Password Recovery Mechanism for Forgotten | 07-10-2019 | 4.3 | SITOS six Build v6.2.1 allows a user to change their password and recovery email address without requiring them to confirm the change with their old password. This would | N/A | A-SIT-SITO-221019/323 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Password | | | allow an attacker with access to the victim's account (e.g., via XSS or an unattended workstation) to change that password and address.<br>**CVE ID : CVE-2019-15749** | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 07-10-2019 | 4.3 | A Cross-Site Scripting (XSS) vulnerability in the blog function in SITOS six Build v6.2.1 allows remote attackers to inject arbitrary web script or HTML via the id parameter.<br>**CVE ID : CVE-2019-15750** | N/A | A-SIT-SITO-221019/324 |
| Unrestricted Upload of File with Dangerous Type | 07-10-2019 | 10 | An unrestricted file upload vulnerability in SITOS six Build v6.2.1 allows remote attackers to execute arbitrary code by uploading a SCORM file with an executable extension. This allows an unauthenticated attacker to upload a malicious file (containing PHP code to execute operating system commands) to the web root of the application.<br>**CVE ID : CVE-2019-15751** | N/A | A-SIT-SITO-221019/325 |
| **snowtide** | | | | | |
| **pdfxstream** | | | | | |
| Improper Input Validation | 01-10-2019 | 4.3 | In Snowtide PDFxStream before 3.7.1 (for Java), a crafted PDF file can trigger an extremely long running computation because of page-tree mishandling.<br>**CVE ID : CVE-2019-17063** | N/A | A-SNO-PDFX-221019/326 |
| **Sugarcrm** | | | | | |
| **sugarcrm** | | | | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 07-10-2019 | 6.5 | SugarCRM before 8.0.4 and 9.x before 9.0.2 allows SQL injection in the pmse_Inbox module by an Admin user. **CVE ID : CVE-2019-17292** | N/A | A-SUG-SUGA-221019/327 |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 07-10-2019 | 6.5 | SugarCRM before 8.0.4 and 9.x before 9.0.2 allows SQL injection in the pmse_Project module by a Regular user. **CVE ID : CVE-2019-17293** | N/A | A-SUG-SUGA-221019/328 |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 07-10-2019 | 6.5 | SugarCRM before 8.0.4 and 9.x before 9.0.2 allows SQL injection in the export function by a Regular user. **CVE ID : CVE-2019-17294** | N/A | A-SUG-SUGA-221019/329 |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 07-10-2019 | 6.5 | SugarCRM before 8.0.4 and 9.x before 9.0.2 allows SQL injection in the history function by a Regular user. **CVE ID : CVE-2019-17295** | N/A | A-SUG-SUGA-221019/330 |
| Improper Neutralization of Special Elements | 07-10-2019 | 6.5 | SugarCRM before 8.0.4 and 9.x before 9.0.2 allows SQL injection in the Contacts module by a Regular user. | N/A | A-SUG-SUGA-221019/331 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| used in an SQL Command ('SQL Injection') | | | **CVE ID : CVE-2019-17296** | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 07-10-2019 | 6.5 | SugarCRM before 8.0.4 and 9.x before 9.0.2 allows SQL injection in the Quotes module by a Regular user.<br>**CVE ID : CVE-2019-17297** | N/A | A-SUG-SUGA-221019/332 |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 07-10-2019 | 6.5 | SugarCRM before 8.0.4 and 9.x before 9.0.2 allows SQL injection in the Administration module by a Developer user.<br>**CVE ID : CVE-2019-17298** | N/A | A-SUG-SUGA-221019/333 |
| Improper Input Validation | 07-10-2019 | 6.5 | SugarCRM before 8.0.4 and 9.x before 9.0.2 allows PHP code injection in the Administration module by an Admin user.<br>**CVE ID : CVE-2019-17299** | N/A | A-SUG-SUGA-221019/334 |
| Improper Input Validation | 07-10-2019 | 6.5 | SugarCRM before 8.0.4 and 9.x before 9.0.2 allows PHP code injection in the Administration module by a Developer user.<br>**CVE ID : CVE-2019-17300** | N/A | A-SUG-SUGA-221019/335 |
| Improper Input Validation | 07-10-2019 | 6.5 | SugarCRM before 8.0.4 and 9.x before 9.0.2 allows PHP code injection in the ModuleBuilder module by an Admin user.<br>**CVE ID : CVE-2019-17301** | N/A | A-SUG-SUGA-221019/336 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Input Validation | 07-10-2019 | 6.5 | SugarCRM before 8.0.4 and 9.x before 9.0.2 allows PHP code injection in the ModuleBuilder module by a Developer user. **CVE ID : CVE-2019-17302** | N/A | A-SUG-SUGA-221019/337 |
| Improper Input Validation | 07-10-2019 | 6.5 | SugarCRM before 8.0.4 and 9.x before 9.0.2 allows PHP code injection in the MergeRecords module by a Developer user. **CVE ID : CVE-2019-17303** | N/A | A-SUG-SUGA-221019/338 |
| Improper Input Validation | 07-10-2019 | 6.5 | SugarCRM before 8.0.4 and 9.x before 9.0.2 allows PHP code injection in the MergeRecords module by an Admin user. **CVE ID : CVE-2019-17304** | N/A | A-SUG-SUGA-221019/339 |
| Improper Input Validation | 07-10-2019 | 6.5 | SugarCRM before 8.0.4 and 9.x before 9.0.2 allows PHP code injection in the MergeRecords module by a Regular user. **CVE ID : CVE-2019-17305** | N/A | A-SUG-SUGA-221019/340 |
| Improper Input Validation | 07-10-2019 | 6.5 | SugarCRM before 8.0.4 and 9.x before 9.0.2 allows PHP code injection in the Configurator module by an Admin user. **CVE ID : CVE-2019-17306** | N/A | A-SUG-SUGA-221019/341 |
| Improper Input Validation | 07-10-2019 | 6.5 | SugarCRM before 8.0.4 and 9.x before 9.0.2 allows PHP code injection in the Tracker module by an Admin user. **CVE ID : CVE-2019-17307** | N/A | A-SUG-SUGA-221019/342 |
| Improper Input Validation | 07-10-2019 | 6.5 | SugarCRM before 8.0.4 and 9.x before 9.0.2 allows PHP code injection in the Emails module by a Regular user. **CVE ID : CVE-2019-17308** | N/A | A-SUG-SUGA-221019/343 |
| Improper Input | 07-10-2019 | 6.5 | SugarCRM before 8.0.4 and 9.x before 9.0.2 allows PHP code | N/A | A-SUG-SUGA- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Validation | | | injection in the EmailMan module by an Admin user.<br>**CVE ID : CVE-2019-17309** | | 221019/344 |
| Improper Input Validation | 07-10-2019 | 6.5 | SugarCRM before 8.0.4 and 9.x before 9.0.2 allows PHP code injection in the Campaigns module by an Admin user.<br>**CVE ID : CVE-2019-17310** | N/A | A-SUG-SUGA-221019/345 |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 07-10-2019 | 6.5 | SugarCRM before 8.0.4 and 9.x before 9.0.2 allows directory traversal in the attachment function by a Regular user.<br>**CVE ID : CVE-2019-17311** | N/A | A-SUG-SUGA-221019/346 |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 07-10-2019 | 6.5 | SugarCRM before 8.0.4 and 9.x before 9.0.2 allows directory traversal in the file function by a Regular user.<br>**CVE ID : CVE-2019-17312** | N/A | A-SUG-SUGA-221019/347 |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 07-10-2019 | 6.5 | SugarCRM before 8.0.4 and 9.x before 9.0.2 allows directory traversal in the Studio module by a Developer user.<br>**CVE ID : CVE-2019-17313** | N/A | A-SUG-SUGA-221019/348 |
| Improper Limitation of a Pathname to a Restricted Directory ('Path | 07-10-2019 | 6.5 | SugarCRM before 8.0.4 and 9.x before 9.0.2 allows directory traversal in the Configurator module by an Admin user.<br>**CVE ID : CVE-2019-17314** | N/A | A-SUG-SUGA-221019/349 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Traversal') | | | | | |
| Improper Input Validation | 07-10-2019 | 6.5 | SugarCRM before 8.0.4 and 9.x before 9.0.2 allows PHP object injection in the Administration module by an Admin user.<br>**CVE ID : CVE-2019-17315** | N/A | A-SUG-SUGA-221019/350 |
| Improper Input Validation | 07-10-2019 | 6.5 | SugarCRM before 8.0.4 and 9.x before 9.0.2 allows PHP object injection in the Import module by a Regular user.<br>**CVE ID : CVE-2019-17316** | N/A | A-SUG-SUGA-221019/351 |
| Improper Input Validation | 07-10-2019 | 6.5 | SugarCRM before 8.0.4 and 9.x before 9.0.2 allows PHP object injection in the UpgradeWizard module by an Admin user.<br>**CVE ID : CVE-2019-17317** | N/A | A-SUG-SUGA-221019/352 |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 07-10-2019 | 6.5 | SugarCRM before 8.0.4 and 9.x before 9.0.2 allows SQL injection in the pmse_Inbox module by a Regular user.<br>**CVE ID : CVE-2019-17318** | N/A | A-SUG-SUGA-221019/353 |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 07-10-2019 | 6.5 | SugarCRM before 8.0.4 and 9.x before 9.0.2 allows SQL injection in the Emails module by a Regular user.<br>**CVE ID : CVE-2019-17319** | N/A | A-SUG-SUGA-221019/354 |
| **Tcpdump** | | | | | |
| **tcpdump** | | | | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Input Validation | 03-10-2019 | 7.5 | lmp_print_data_link_subobjs() in print-lmp.c in tcpdump before 4.9.3 lacks certain bounds checks.<br>**CVE ID : CVE-2019-15166** | https://github.com/the-tcpdump-group/tcpdump/commit/0b661e0aa61850234b64394585cf577aac570bf4 | A-TCP-TCPD-221019/355 |
| **libpcap** | | | | | |
| Improper Input Validation | 03-10-2019 | 5 | rpcapd/daemon.c in libpcap before 1.9.1 mishandles certain length values because of reuse of a variable. This may open up an attack vector involving extra data at the end of a request.<br>**CVE ID : CVE-2019-15161** | https://github.com/the-tcpdump-group/libpcap/blob/libpcap-1.9/CHANGES, https://github.com/the-tcpdump-group/libpcap/commit/617b12c0339db4891d117b661982126c495439ea, https://www.tcpdump.org/public-cve-list.txt | A-TCP-LIBP-221019/356 |
| Insufficient Verification of Data | 03-10-2019 | 5 | rpcapd/daemon.c in libpcap before 1.9.1 on non-Windows platforms provides details | https://github.com/the- | A-TCP-LIBP-221019/357 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Authenticity | | | about why authentication failed, which might make it easier for attackers to enumerate valid usernames.<br>**CVE ID : CVE-2019-15162** | tcpdump-group/libpcap/blob/libpcap-1.9/CHANGES, https://github.com/the-tcpdump-group/libpcap/commit/484d60cbf7ca4ec758c3cbb8a82d68b244a78d58, https://www.tcpdump.org/public-cve-list.txt | |
| NULL Pointer Dereference | 03-10-2019 | 5 | rpcapd/daemon.c in libpcap before 1.9.1 allows attackers to cause a denial of service (NULL pointer dereference and daemon crash) if a crypt() call fails.<br>**CVE ID : CVE-2019-15163** | https://github.com/the-tcpdump-group/libpcap/blob/libpcap-1.9/CHANGES, https://github.com/the-tcpdump-group/libpcap/commit/437b273761adedcbd880f714bfa44afeec1 | A-TCP-LIBP-221019/358 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | 86a31, https://www.tcpdump.org/public-cve-list.txt | |
| Server-Side Request Forgery (SSRF) | 03-10-2019 | 5 | rpcapd/daemon.c in libpcap before 1.9.1 allows SSRF because a URL may be provided as a capture source. **CVE ID : CVE-2019-15164** | https://github.com/the-tcpdump-group/libpcap/blob/libpcap-1.9/CHANGES, https://github.com/the-tcpdump-group/libpcap/commit/33834cb2a4d035b52aa2a26742f832a112e90a0a, https://www.tcpdump.org/public-cve-list.txt | A-TCP-LIBP-221019/359 |
| Improper Input Validation | 03-10-2019 | 5 | sf-pcapng.c in libpcap before 1.9.1 does not properly validate the PHB header length before allocating memory. **CVE ID : CVE-2019-15165** | https://github.com/the-tcpdump-group/libpcap/blob/libpcap-1.9/CHANGES, https://git | A-TCP-LIBP-221019/360 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | hub.com/the-tcpdump-group/libpcap/commit/87d6bef033062f969e70fa40c43dfd945d5a20ab, https://www.tcpdump.org/public-cve-list.txt | |
| **Teampass** | | | | | |
| **teampass** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 05-10-2019 | 3.5 | TeamPass 2.1.27.36 allows Stored XSS at the Search page by setting a crafted password for an item in any folder. **CVE ID : CVE-2019-17203** | N/A | A-TEA-TEAM-221019/361 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 05-10-2019 | 3.5 | TeamPass 2.1.27.36 allows Stored XSS by setting a crafted Knowledge Base label and adding any available item. **CVE ID : CVE-2019-17204** | N/A | A-TEA-TEAM-221019/362 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site | 05-10-2019 | 4.3 | TeamPass 2.1.27.36 allows Stored XSS by placing a payload in the username field during a login attempt. When an administrator looks at the log of failed logins, the XSS | N/A | A-TEA-TEAM-221019/363 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Scripting') | | | payload will be executed.<br>**CVE ID : CVE-2019-17205** | | |
| **themeisle** | | | | | |
| **visualizer** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 03-10-2019 | 4.3 | A stored XSS vulnerability in the Visualizer plugin 3.3.0 for WordPress allows an unauthenticated attacker to execute arbitrary JavaScript when an admin or other privileged user edits the chart via the admin dashboard. This occurs because classes/Visualizer/Gutenberg/Block.php registers wp-json/visualizer/v1/update-chart with no access control, and classes/Visualizer/Render/Page/Data.php lacks output sanitization.<br>**CVE ID : CVE-2019-16931** | N/A | A-THE-VISU-221019/364 |
| **Tibco** | | | | | |
| **master_data_management** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 09-10-2019 | 3.5 | The MDM server component of TIBCO Software Inc's TIBCO MDM contains multiple vulnerabilities that theoretically allow an authenticated user with specific roles to perform cross-site scripting (XSS) attacks. This issue affects TIBCO Software Inc.'s TIBCO MDM version 9.0.1 and prior versions; version 9.1.0.<br>**CVE ID : CVE-2019-11212** | http://www.tibco.com/services/support/advisories, https://www.tibco.com/support/advisories/2019/10/tibco-security-advisory-october-8-2019- | A-TIB-MAST-221019/365 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | tibco-mdm | |
| **Twitter** | | | | | |
| **twitter_kit** | | | | | |
| Improper Certificate Validation | 07-10-2019 | 5.8 | The Twitter Kit framework through 3.4.2 for iOS does not properly validate the api.twitter.com SSL certificate. Although the certificate chain must contain one of a set of pinned certificates, there are certain implementation errors such as a lack of hostname verification. NOTE: this is an end-of-life product. **CVE ID : CVE-2019-16263** | N/A | A-TWI-TWIT-221019/366 |
| **Umbraco** | | | | | |
| **umbraco** | | | | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 02-10-2019 | 7.5 | In Umbraco 7.3.8, there is SQL Injection in the backoffice/PageWApprove/PageWApproveApi/GetInpectSearch method via the nodeName parameter. **CVE ID : CVE-2019-13957** | N/A | A-UMB-UMBR-221019/367 |
| **vanderbilt** | | | | | |
| **redcap** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 04-10-2019 | 3.5 | REDCap before 9.3.4 has XSS on the Customize & Manage Locking/E-signatures page via Lock Record Custom Text values. **CVE ID : CVE-2019-17121** | N/A | A-VAN-REDC-221019/368 |
| **Vbulletin** | | | | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **vbulletin** | | | | | |
| Files or Directories Accessible to External Parties | 04-10-2019 | 6.4 | vBulletin through 5.5.4 mishandles external URLs within the /core/vb/vurl.php file and the /core/vb/vurl directories.<br>**CVE ID : CVE-2019-17130** | N/A | A-VBU-VBUL-221019/369 |
| Improper Restriction of Rendered UI Layers or Frames | 04-10-2019 | 4.3 | vBulletin before 5.5.4 allows clickjacking.<br>**CVE ID : CVE-2019-17131** | N/A | A-VBU-VBUL-221019/370 |
| Improper Input Validation | 04-10-2019 | 6.8 | vBulletin through 5.5.4 mishandles custom avatars.<br>**CVE ID : CVE-2019-17132** | N/A | A-VBU-VBUL-221019/371 |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 08-10-2019 | 4 | vBulletin 5.5.4 allows SQL Injection via the ajax/api/hook/getHookList or ajax/api/widget/getWidgetList where parameter.<br>**CVE ID : CVE-2019-17271** | N/A | A-VBU-VBUL-221019/372 |
| **webarxsecurity** | | | | | |
| **webarx** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 06-10-2019 | 4.3 | The WebARX plugin 1.3.0 for WordPress has unauthenticated stored XSS via the URI or the X-Forwarded-For HTTP header.<br>**CVE ID : CVE-2019-17213** | N/A | A-WEB-WEBA-221019/373 |
| Incorrect Authorization | 06-10-2019 | 5 | The WebARX plugin 1.3.0 for WordPress allows firewall bypass by appending &cc=1 to a URI. | N/A | A-WEB-WEBA-221019/374 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2019-17214** | | |
| **webpagetest** | | | | | |
| **webpagetest** | | | | | |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 05-10-2019 | 5 | www/getfile.php in WPO WebPageTest 19.04 on Windows allows Directory Traversal (for reading arbitrary files) because of an unanchored regular expression, as demonstrated by the a.jpg\.. substring.<br>**CVE ID : CVE-2019-17199** | N/A | A-WEB-WEBP-221019/375 |
| **whatsapp** | | | | | |
| **whatsapp** | | | | | |
| Double Free | 03-10-2019 | 7.5 | A double free vulnerability in the DDGifSlurp function in decoding.c in libpl_droidsonroids_gif before 1.2.15, as used in WhatsApp for Android before 2.19.244, allows remote attackers to execute arbitrary code or cause a denial of service.<br>**CVE ID : CVE-2019-11932** | https://www.facebook.com/security/advisories/cve-2019-11932 | A-WHA-WHAT-221019/376 |
| **Wolfssl** | | | | | |
| **wolfssl** | | | | | |
| Information Exposure Through Discrepancy | 03-10-2019 | 1.2 | wolfSSL and wolfCrypt 4.0.0 and earlier (when configured without --enable-fpecc, --enable-sp, or --enable-sp-math) contain a timing side channel in ECDSA signature generation. This allows a local attacker, able to precisely measure the duration of signature operations, to infer information about the nonces used and potentially mount a | N/A | A-WOL-WOLF-221019/377 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | lattice attack to recover the private key used. The issue occurs because ecc.c scalar multiplication might leak the bit length.<br>**CVE ID : CVE-2019-13628** | | |
| **wpfactory** | | | | | |
| **download_plugins_and_themes_from_dashboard** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 07-10-2019 | 4.3 | includes/settings/class-alg-download-plugins-settings.php in the download-plugins-dashboard plugin through 1.5.0 for WordPress has multiple unauthenticated stored XSS issues.<br>**CVE ID : CVE-2019-17239** | N/A | A-WPF-DOWN-221019/378 |
| **Xnview** | | | | | |
| **xnview** | | | | | |
| Out-of-bounds Write | 08-10-2019 | 4.6 | XnView Classic 2.49.1 allows a User Mode Write AV starting at Xwsq+0x0000000000001e51.<br>**CVE ID : CVE-2019-17261** | N/A | A-XNV-XNVI-221019/379 |
| Out-of-bounds Write | 08-10-2019 | 4.6 | XnView Classic 2.49.1 allows a User Mode Write AV starting at Xwsq+0x0000000000001fc0.<br>**CVE ID : CVE-2019-17262** | N/A | A-XNV-XNVI-221019/380 |
| **xunruicms** | | | | | |
| **xunruicms** | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site | 01-10-2019 | 3.5 | An issue was discovered in XunRuiCMS 4.3.1. There is a stored XSS in the module_category area.<br>**CVE ID : CVE-2019-17074** | N/A | A-XUN-XUNR-221019/381 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Scripting') | | | | | |
| **zingbox** | | | | | |
| **inspector** | | | | | |
| Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') | 09-10-2019 | 9 | A command injection vulnerability exists in the Zingbox Inspector versions 1.286 and earlier, that allows for an authenticated user to execute arbitrary system commands in the CLI.<br>**CVE ID : CVE-2019-15014** | N/A | A-ZIN-INSP-221019/382 |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 09-10-2019 | 6.5 | An SQL injection vulnerability exists in the management interface of Zingbox Inspector versions 1.288 and earlier, that allows for unsanitized data provided by an authenticated user to be passed from the web UI into the database.<br>**CVE ID : CVE-2019-15016** | N/A | A-ZIN-INSP-221019/383 |
| Improper Authentication | 09-10-2019 | 5 | A security vulnerability exists in the Zingbox Inspector versions 1.280 and earlier, where authentication is not required when binding the Inspector instance to a different customer tenant.<br>**CVE ID : CVE-2019-15018** | N/A | A-ZIN-INSP-221019/384 |
| Improper Input Validation | 09-10-2019 | 7.5 | A security vulnerability exists in the Zingbox Inspector versions 1.294 and earlier, that could allow an attacker to supply an invalid software update image to the Zingbox Inspector.<br>**CVE ID : CVE-2019-15019** | N/A | A-ZIN-INSP-221019/385 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') | 09-10-2019 | 7.5 | A security vulnerability exists in the Zingbox Inspector versions 1.293 and earlier, that could allow an attacker to supply an invalid software update image to the Zingbox Inspector that could result in command injection. **CVE ID : CVE-2019-15020** | N/A | A-ZIN-INSP-221019/386 |
| Information Exposure | 09-10-2019 | 5 | A security vulnerability exists in the Zingbox Inspector versions 1.294 and earlier, that can allow an attacker to easily identify instances of Zingbox Inspectors in a local area network. **CVE ID : CVE-2019-15021** | N/A | A-ZIN-INSP-221019/387 |
| Authentication Bypass by Spoofing | 09-10-2019 | 5 | A security vulnerability exists in Zingbox Inspector versions 1.294 and earlier, that allows for the Inspector to be susceptible to ARP spoofing. **CVE ID : CVE-2019-15022** | N/A | A-ZIN-INSP-221019/388 |
| Cleartext Storage of Sensitive Information | 09-10-2019 | 5 | A security vulnerability exists in Zingbox Inspector versions 1.294 and earlier, that results in passwords for 3rd party integrations being stored in cleartext in device configuration. **CVE ID : CVE-2019-15023** | N/A | A-ZIN-INSP-221019/389 |
| Improper Input Validation | 09-10-2019 | 6.8 | A security vulnerability exists in Zingbox Inspector version 1.293 and earlier, that allows for remote code execution if the Inspector were sent a malicious command from the Zingbox cloud, or if the Zingbox Inspector were | N/A | A-ZIN-INSP-221019/390 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | tampered with to connect to an attacker's cloud endpoint.<br>**CVE ID : CVE-2019-1584** | | |
| **Zohocorp** | | | | | |
| **manageengine_datasecurity_plus** | | | | | |
| Files or Directories Accessible to External Parties | 09-10-2019 | 4 | An issue was discovered in Zoho ManageEngine DataSecurity Plus before 5.0.1 5012. An exposed service allows a basic user ("Operator" access level) to access the configuration file of the mail server (except for the password).<br>**CVE ID : CVE-2019-17112** | N/A | A-ZOH-MANA-221019/391 |
| **Operating System** | | | | | |
| **Canonical** | | | | | |
| **ubuntu_linux** | | | | | |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 03-10-2019 | 5 | Unbound before 1.9.4 accesses uninitialized memory, which allows remote attackers to trigger a crash via a crafted NOTIFY query. The source IP address of the query must match an access-control rule.<br>**CVE ID : CVE-2019-16866** | N/A | O-CAN-UBUN-221019/392 |
| Out-of-bounds Read | 06-10-2019 | 7.5 | libsoup from versions 2.65.1 until 2.68.1 have a heap-based buffer over-read because soup_ntlm_parse_challenge() in soup-auth-ntlm.c does not properly check an NTLM message's length before proceeding with a memcpy.<br>**CVE ID : CVE-2019-17266** | N/A | O-CAN-UBUN-221019/393 |
| **Checkpoint** | | | | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **gaia** | | | | | |
| Improper Handling of Exceptional Conditions | 02-10-2019 | 5 | In a rare scenario, Check Point R80.30 Security Gateway before JHF Take 50 managed by Check Point R80.30 Management crashes with a unique configuration of enhanced logging.<br>**CVE ID : CVE-2019-8462** | N/A | O-CHE-GAIA-221019/394 |
| **Cisco** | | | | | |
| **firepower_9300_firmware** | | | | | |
| Improper Encoding or Escaping of Output | 02-10-2019 | 7.2 | Multiple vulnerabilities in the multi-instance feature of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to escape the container for their FTD instance and execute commands with root privileges in the host namespace. These vulnerabilities are due to insufficient protections on the underlying filesystem. An attacker could exploit these vulnerabilities by modifying critical files on the underlying filesystem. A successful exploit could allow the attacker to execute commands with root privileges within the host namespace. This could allow the attacker to impact other running FTD instances.<br>**CVE ID : CVE-2019-12674** | N/A | O-CIS-FIRE-221019/395 |
| Improper Encoding or Escaping of Output | 02-10-2019 | 7.2 | Multiple vulnerabilities in the multi-instance feature of Cisco Firepower Threat Defense (FTD) Software could allow an | N/A | O-CIS-FIRE-221019/396 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | authenticated, local attacker to escape the container for their FTD instance and execute commands with root privileges in the host namespace. These vulnerabilities are due to insufficient protections on the underlying filesystem. An attacker could exploit these vulnerabilities by modifying critical files on the underlying filesystem. A successful exploit could allow the attacker to execute commands with root privileges within the host namespace. This could allow the attacker to impact other running FTD instances.<br>**CVE ID : CVE-2019-12675** | | |
| Improper Input Validation | 02-10-2019 | 7.2 | Multiple vulnerabilities in the CLI of Cisco FXOS Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute commands on the underlying operating system (OS) with root privileges. These vulnerabilities are due to insufficient input validation. An attacker could exploit these vulnerabilities by including crafted arguments to specific CLI commands. A successful exploit could allow the attacker to execute commands on the underlying OS with root privileges.<br>**CVE ID : CVE-2019-12699** | N/A | O-CIS-FIRE-221019/397 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Uncontrolled Resource Consumption | 02-10-2019 | 6.8 | A vulnerability in the configuration of the Pluggable Authentication Module (PAM) used in Cisco Firepower Threat Defense (FTD) Software, Cisco Firepower Management Center (FMC) Software, and Cisco FXOS Software could allow an authenticated, remote attacker to cause a denial of service (DoS) condition. The vulnerability is due to improper resource management in the context of user session management. An attacker could exploit this vulnerability by connecting to an affected system and performing many simultaneous successful Secure Shell (SSH) logins. A successful exploit could allow the attacker to exhaust system resources and cause the device to reload, resulting in a DoS condition. To exploit this vulnerability, the attacker needs valid user credentials on the system.<br>**CVE ID : CVE-2019-12700** | N/A | O-CIS-FIRE-221019/398 |
| **firepower_4115_firmware** | | | | | |
| Improper Encoding or Escaping of Output | 02-10-2019 | 7.2 | Multiple vulnerabilities in the multi-instance feature of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to escape the container for their FTD instance and execute commands with root | N/A | O-CIS-FIRE-221019/399 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | privileges in the host namespace. These vulnerabilities are due to insufficient protections on the underlying filesystem. An attacker could exploit these vulnerabilities by modifying critical files on the underlying filesystem. A successful exploit could allow the attacker to execute commands with root privileges within the host namespace. This could allow the attacker to impact other running FTD instances.<br>**CVE ID : CVE-2019-12674** | | |
| Improper Encoding or Escaping of Output | 02-10-2019 | 7.2 | Multiple vulnerabilities in the multi-instance feature of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to escape the container for their FTD instance and execute commands with root privileges in the host namespace. These vulnerabilities are due to insufficient protections on the underlying filesystem. An attacker could exploit these vulnerabilities by modifying critical files on the underlying filesystem. A successful exploit could allow the attacker to execute commands with root privileges within the host namespace. This could allow the attacker to impact other running FTD instances.<br>**CVE ID : CVE-2019-12675** | N/A | O-CIS-FIRE-221019/400 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **firepower_4125_firmware** | | | | | |
| Improper Encoding or Escaping of Output | 02-10-2019 | 7.2 | Multiple vulnerabilities in the multi-instance feature of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to escape the container for their FTD instance and execute commands with root privileges in the host namespace. These vulnerabilities are due to insufficient protections on the underlying filesystem. An attacker could exploit these vulnerabilities by modifying critical files on the underlying filesystem. A successful exploit could allow the attacker to execute commands with root privileges within the host namespace. This could allow the attacker to impact other running FTD instances.<br>**CVE ID : CVE-2019-12674** | N/A | O-CIS-FIRE-221019/401 |
| Improper Encoding or Escaping of Output | 02-10-2019 | 7.2 | Multiple vulnerabilities in the multi-instance feature of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to escape the container for their FTD instance and execute commands with root privileges in the host namespace. These vulnerabilities are due to insufficient protections on the underlying filesystem. An attacker could exploit these vulnerabilities by modifying | N/A | O-CIS-FIRE-221019/402 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | critical files on the underlying filesystem. A successful exploit could allow the attacker to execute commands with root privileges within the host namespace. This could allow the attacker to impact other running FTD instances.<br>**CVE ID : CVE-2019-12675** | | |
| **firepower_4145_firmware** | | | | | |
| Improper Encoding or Escaping of Output | 02-10-2019 | 7.2 | Multiple vulnerabilities in the multi-instance feature of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to escape the container for their FTD instance and execute commands with root privileges in the host namespace. These vulnerabilities are due to insufficient protections on the underlying filesystem. An attacker could exploit these vulnerabilities by modifying critical files on the underlying filesystem. A successful exploit could allow the attacker to execute commands with root privileges within the host namespace. This could allow the attacker to impact other running FTD instances.<br>**CVE ID : CVE-2019-12674** | N/A | O-CIS-FIRE-221019/403 |
| Improper Encoding or Escaping of Output | 02-10-2019 | 7.2 | Multiple vulnerabilities in the multi-instance feature of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to escape the container for their | N/A | O-CIS-FIRE-221019/404 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | FTD instance and execute commands with root privileges in the host namespace. These vulnerabilities are due to insufficient protections on the underlying filesystem. An attacker could exploit these vulnerabilities by modifying critical files on the underlying filesystem. A successful exploit could allow the attacker to execute commands with root privileges within the host namespace. This could allow the attacker to impact other running FTD instances.<br>**CVE ID : CVE-2019-12675** | | |
| **firepower_4110_firmware** | | | | | |
| Improper Encoding or Escaping of Output | 02-10-2019 | 7.2 | Multiple vulnerabilities in the multi-instance feature of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to escape the container for their FTD instance and execute commands with root privileges in the host namespace. These vulnerabilities are due to insufficient protections on the underlying filesystem. An attacker could exploit these vulnerabilities by modifying critical files on the underlying filesystem. A successful exploit could allow the attacker to execute commands with root privileges within the host namespace. This could allow | N/A | O-CIS-FIRE-221019/405 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | the attacker to impact other running FTD instances.<br>**CVE ID : CVE-2019-12674** | | |
| Improper Encoding or Escaping of Output | 02-10-2019 | 7.2 | Multiple vulnerabilities in the multi-instance feature of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to escape the container for their FTD instance and execute commands with root privileges in the host namespace. These vulnerabilities are due to insufficient protections on the underlying filesystem. An attacker could exploit these vulnerabilities by modifying critical files on the underlying filesystem. A successful exploit could allow the attacker to execute commands with root privileges within the host namespace. This could allow the attacker to impact other running FTD instances.<br>**CVE ID : CVE-2019-12675** | N/A | O-CIS-FIRE-221019/406 |
| **firepower_4120_firmware** | | | | | |
| Improper Encoding or Escaping of Output | 02-10-2019 | 7.2 | Multiple vulnerabilities in the multi-instance feature of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to escape the container for their FTD instance and execute commands with root privileges in the host namespace. These vulnerabilities are due to insufficient protections on the | N/A | O-CIS-FIRE-221019/407 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | underlying filesystem. An attacker could exploit these vulnerabilities by modifying critical files on the underlying filesystem. A successful exploit could allow the attacker to execute commands with root privileges within the host namespace. This could allow the attacker to impact other running FTD instances.<br>**CVE ID : CVE-2019-12674** | | |
| Improper Encoding or Escaping of Output | 02-10-2019 | 7.2 | Multiple vulnerabilities in the multi-instance feature of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to escape the container for their FTD instance and execute commands with root privileges in the host namespace. These vulnerabilities are due to insufficient protections on the underlying filesystem. An attacker could exploit these vulnerabilities by modifying critical files on the underlying filesystem. A successful exploit could allow the attacker to execute commands with root privileges within the host namespace. This could allow the attacker to impact other running FTD instances.<br>**CVE ID : CVE-2019-12675** | N/A | O-CIS-FIRE-221019/408 |
| **firepower_4140_firmware** | | | | | |
| Improper Encoding or Escaping of | 02-10-2019 | 7.2 | Multiple vulnerabilities in the multi-instance feature of Cisco Firepower Threat Defense | N/A | O-CIS-FIRE-221019/409 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Output | | | (FTD) Software could allow an authenticated, local attacker to escape the container for their FTD instance and execute commands with root privileges in the host namespace. These vulnerabilities are due to insufficient protections on the underlying filesystem. An attacker could exploit these vulnerabilities by modifying critical files on the underlying filesystem. A successful exploit could allow the attacker to execute commands with root privileges within the host namespace. This could allow the attacker to impact other running FTD instances.<br>**CVE ID : CVE-2019-12674** | | |
| Improper Encoding or Escaping of Output | 02-10-2019 | 7.2 | Multiple vulnerabilities in the multi-instance feature of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to escape the container for their FTD instance and execute commands with root privileges in the host namespace. These vulnerabilities are due to insufficient protections on the underlying filesystem. An attacker could exploit these vulnerabilities by modifying critical files on the underlying filesystem. A successful exploit could allow the attacker to execute commands with root privileges within the host | N/A | O-CIS-FIRE-221019/410 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | namespace. This could allow the attacker to impact other running FTD instances.<br>**CVE ID : CVE-2019-12675** | | |
| **firepower_4150_firmware** | | | | | |
| Improper Encoding or Escaping of Output | 02-10-2019 | 7.2 | Multiple vulnerabilities in the multi-instance feature of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to escape the container for their FTD instance and execute commands with root privileges in the host namespace. These vulnerabilities are due to insufficient protections on the underlying filesystem. An attacker could exploit these vulnerabilities by modifying critical files on the underlying filesystem. A successful exploit could allow the attacker to execute commands with root privileges within the host namespace. This could allow the attacker to impact other running FTD instances.<br>**CVE ID : CVE-2019-12674** | N/A | O-CIS-FIRE-221019/411 |
| Improper Encoding or Escaping of Output | 02-10-2019 | 7.2 | Multiple vulnerabilities in the multi-instance feature of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to escape the container for their FTD instance and execute commands with root privileges in the host namespace. These vulnerabilities are due to | N/A | O-CIS-FIRE-221019/412 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | insufficient protections on the underlying filesystem. An attacker could exploit these vulnerabilities by modifying critical files on the underlying filesystem. A successful exploit could allow the attacker to execute commands with root privileges within the host namespace. This could allow the attacker to impact other running FTD instances.<br>**CVE ID : CVE-2019-12675** | | |
| **fxos** | | | | | |
| Improper Input Validation | 02-10-2019 | 7.2 | Multiple vulnerabilities in the CLI of Cisco FXOS Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute commands on the underlying operating system (OS) with root privileges. These vulnerabilities are due to insufficient input validation. An attacker could exploit these vulnerabilities by including crafted arguments to specific CLI commands. A successful exploit could allow the attacker to execute commands on the underlying OS with root privileges.<br>**CVE ID : CVE-2019-12699** | N/A | O-CIS-FXOS-221019/413 |
| Uncontrolled Resource Consumption | 02-10-2019 | 6.8 | A vulnerability in the configuration of the Pluggable Authentication Module (PAM) used in Cisco Firepower Threat Defense (FTD) Software, Cisco Firepower | N/A | O-CIS-FXOS-221019/414 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Management Center (FMC) Software, and Cisco FXOS Software could allow an authenticated, remote attacker to cause a denial of service (DoS) condition. The vulnerability is due to improper resource management in the context of user session management. An attacker could exploit this vulnerability by connecting to an affected system and performing many simultaneous successful Secure Shell (SSH) logins. A successful exploit could allow the attacker to exhaust system resources and cause the device to reload, resulting in a DoS condition. To exploit this vulnerability, the attacker needs valid user credentials on the system.<br>**CVE ID : CVE-2019-12700** | | |
| **email_security_appliance_firmware** | | | | | |
| Improper Input Validation | 02-10-2019 | 5 | A vulnerability in the Sender Policy Framework (SPF) functionality of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to bypass the configured user filters on an affected device. The vulnerability exists because the affected software insufficiently validates certain incoming SPF messages. An attacker could exploit this | N/A | O-CIS-EMAI-221019/415 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | vulnerability by sending a custom SPF packet to an affected device. A successful exploit could allow the attacker to bypass the configured header filters, which could allow malicious content to pass through the device.<br>**CVE ID : CVE-2019-12706** | | |
| **ic3000_industrial_compute_gateway_firmware** | | | | | |
| Uncontrolled Resource Consumption | 02-10-2019 | 4 | A vulnerability in the web-based management interface of Cisco IC3000 Industrial Compute Gateway could allow an authenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability exists because the affected software improperly manages system resources. An attacker could exploit this vulnerability by opening a large number of simultaneous sessions on the web-based management interface of an affected device. A successful exploit could allow the attacker to cause a DoS condition of the web-based management interface, preventing normal management operations.<br>**CVE ID : CVE-2019-12714** | N/A | O-CIS-IC30-221019/416 |
| **asa_5505_firmware** | | | | | |
| Uncontrolled Resource Consumption | 02-10-2019 | 7.8 | A vulnerability in the Internet Key Exchange version 1 (IKEv1) feature of Cisco | N/A | O-CIS-ASA_-221019/417 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to improper management of system memory. An attacker could exploit this vulnerability by sending malicious IKEv1 traffic to an affected device. The attacker does not need valid credentials to authenticate the VPN session, nor does the attacker's source address need to match a peer statement in the crypto map applied to the ingress interface of the affected device. An exploit could allow the attacker to exhaust system memory resources, leading to a reload of an affected device.<br>**CVE ID : CVE-2019-15256** | | |
| **asa_5510_firmware** | | | | | |
| Uncontrolled Resource Consumption | 02-10-2019 | 7.8 | A vulnerability in the Internet Key Exchange version 1 (IKEv1) feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is | N/A | O-CIS-ASA_-221019/418 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | due to improper management of system memory. An attacker could exploit this vulnerability by sending malicious IKEv1 traffic to an affected device. The attacker does not need valid credentials to authenticate the VPN session, nor does the attacker's source address need to match a peer statement in the crypto map applied to the ingress interface of the affected device. An exploit could allow the attacker to exhaust system memory resources, leading to a reload of an affected device.<br>**CVE ID : CVE-2019-15256** | | |
| **asa_5512-x_firmware** | | | | | |
| Uncontrolled Resource Consumption | 02-10-2019 | 7.8 | A vulnerability in the Internet Key Exchange version 1 (IKEv1) feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to improper management of system memory. An attacker could exploit this vulnerability by sending malicious IKEv1 traffic to an affected device. The attacker does not need valid credentials to authenticate the VPN session, nor does the attacker's source | N/A | O-CIS-ASA_-221019/419 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | address need to match a peer statement in the crypto map applied to the ingress interface of the affected device. An exploit could allow the attacker to exhaust system memory resources, leading to a reload of an affected device.<br>**CVE ID : CVE-2019-15256** | | |
| **asa_5515-x_firmware** | | | | | |
| Uncontrolled Resource Consumption | 02-10-2019 | 7.8 | A vulnerability in the Internet Key Exchange version 1 (IKEv1) feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to improper management of system memory. An attacker could exploit this vulnerability by sending malicious IKEv1 traffic to an affected device. The attacker does not need valid credentials to authenticate the VPN session, nor does the attacker's source address need to match a peer statement in the crypto map applied to the ingress interface of the affected device. An exploit could allow the attacker to exhaust system memory resources, leading to a reload of an affected device.<br>**CVE ID : CVE-2019-15256** | N/A | O-CIS-ASA_-221019/420 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **asa_5520_firmware** | | | | | |
| Uncontrolled Resource Consumption | 02-10-2019 | 7.8 | A vulnerability in the Internet Key Exchange version 1 (IKEv1) feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to improper management of system memory. An attacker could exploit this vulnerability by sending malicious IKEv1 traffic to an affected device. The attacker does not need valid credentials to authenticate the VPN session, nor does the attacker's source address need to match a peer statement in the crypto map applied to the ingress interface of the affected device. An exploit could allow the attacker to exhaust system memory resources, leading to a reload of an affected device.<br>**CVE ID : CVE-2019-15256** | N/A | O-CIS-ASA_-221019/421 |
| **asa_5525-x_firmware** | | | | | |
| Uncontrolled Resource Consumption | 02-10-2019 | 7.8 | A vulnerability in the Internet Key Exchange version 1 (IKEv1) feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote | N/A | O-CIS-ASA_-221019/422 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | attacker to trigger a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to improper management of system memory. An attacker could exploit this vulnerability by sending malicious IKEv1 traffic to an affected device. The attacker does not need valid credentials to authenticate the VPN session, nor does the attacker's source address need to match a peer statement in the crypto map applied to the ingress interface of the affected device. An exploit could allow the attacker to exhaust system memory resources, leading to a reload of an affected device.<br>**CVE ID : CVE-2019-15256** | | |
| **asa_5540_firmware** | | | | | |
| Uncontrolled Resource Consumption | 02-10-2019 | 7.8 | A vulnerability in the Internet Key Exchange version 1 (IKEv1) feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to improper management of system memory. An attacker could exploit this vulnerability by sending malicious IKEv1 traffic to an affected device. | N/A | O-CIS-ASA_-221019/423 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | The attacker does not need valid credentials to authenticate the VPN session, nor does the attacker's source address need to match a peer statement in the crypto map applied to the ingress interface of the affected device. An exploit could allow the attacker to exhaust system memory resources, leading to a reload of an affected device.<br>**CVE ID : CVE-2019-15256** | | |
| **asa_5545-x_firmware** | | | | | |
| Uncontrolled Resource Consumption | 02-10-2019 | 7.8 | A vulnerability in the Internet Key Exchange version 1 (IKEv1) feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to improper management of system memory. An attacker could exploit this vulnerability by sending malicious IKEv1 traffic to an affected device. The attacker does not need valid credentials to authenticate the VPN session, nor does the attacker's source address need to match a peer statement in the crypto map applied to the ingress interface of the affected device. An exploit could allow the | N/A | O-CIS-ASA_-221019/424 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | attacker to exhaust system memory resources, leading to a reload of an affected device.<br>**CVE ID : CVE-2019-15256** | | |
| **asa_5550_firmware** | | | | | |
| Uncontrolled Resource Consumption | 02-10-2019 | 7.8 | A vulnerability in the Internet Key Exchange version 1 (IKEv1) feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to improper management of system memory. An attacker could exploit this vulnerability by sending malicious IKEv1 traffic to an affected device. The attacker does not need valid credentials to authenticate the VPN session, nor does the attacker's source address need to match a peer statement in the crypto map applied to the ingress interface of the affected device. An exploit could allow the attacker to exhaust system memory resources, leading to a reload of an affected device.<br>**CVE ID : CVE-2019-15256** | N/A | O-CIS-ASA_-221019/425 |
| **asa_5555-x_firmware** | | | | | |
| Uncontrolled Resource Consumption | 02-10-2019 | 7.8 | A vulnerability in the Internet Key Exchange version 1 (IKEv1) feature of Cisco | N/A | O-CIS-ASA_-221019/426 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to improper management of system memory. An attacker could exploit this vulnerability by sending malicious IKEv1 traffic to an affected device. The attacker does not need valid credentials to authenticate the VPN session, nor does the attacker's source address need to match a peer statement in the crypto map applied to the ingress interface of the affected device. An exploit could allow the attacker to exhaust system memory resources, leading to a reload of an affected device.<br>**CVE ID : CVE-2019-15256** | | |
| **asa_5580_firmware** | | | | | |
| Uncontrolled Resource Consumption | 02-10-2019 | 7.8 | A vulnerability in the Internet Key Exchange version 1 (IKEv1) feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is | N/A | O-CIS-ASA_-221019/427 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | due to improper management of system memory. An attacker could exploit this vulnerability by sending malicious IKEv1 traffic to an affected device. The attacker does not need valid credentials to authenticate the VPN session, nor does the attacker's source address need to match a peer statement in the crypto map applied to the ingress interface of the affected device. An exploit could allow the attacker to exhaust system memory resources, leading to a reload of an affected device.<br>**CVE ID : CVE-2019-15256** | | |
| **compal** | | | | | |
| **ch7465lg_firmware** | | | | | |
| Improper Input Validation | 02-10-2019 | 7.5 | Compal CH7465LG CH7465LG-NCIP-6.12.18.24-5p8-NOSH devices have Incorrect Access Control because of Improper Input Validation. The attacker can send a maliciously modified POST (HTTP) request containing shell commands, which will be executed on the device, to an backend API endpoint of the cable modem.<br>**CVE ID : CVE-2019-13025** | N/A | O-COM-CH74-221019/428 |
| **Debian** | | | | | |
| **debian_linux** | | | | | |
| Improper Input Validation | 01-10-2019 | 7.5 | A Polymorphic Typing issue was discovered in FasterXML jackson-databind 2.0.0 through 2.9.10. When Default Typing is enabled (either | N/A | O-DEB-DEBI-221019/429 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | globally or for a specific property) for an externally exposed JSON endpoint and the service has the commons-dbcp (1.4) jar in the classpath, and an attacker can find an RMI service endpoint to access, it is possible to make the service execute a malicious payload. This issue exists because of org.apache.commons.dbcp.datasources.SharedPoolDataSource and org.apache.commons.dbcp.datasources.PerUserPoolDataSource mishandling.<br>**CVE ID : CVE-2019-16942** | | |
| Improper Input Validation | 01-10-2019 | 7.5 | A Polymorphic Typing issue was discovered in FasterXML jackson-databind 2.0.0 through 2.9.10. When Default Typing is enabled (either globally or for a specific property) for an externally exposed JSON endpoint and the service has the p6spy (3.8.6) jar in the classpath, and an attacker can find an RMI service endpoint to access, it is possible to make the service execute a malicious payload. This issue exists because of com.p6spy.engine.spy.P6DataSource mishandling.<br>**CVE ID : CVE-2019-16943** | N/A | O-DEB-DEBI-221019/430 |
| **fiberhome** | | | | | |
| **hg2201t_firmware** | | | | | |
| Improper | 08-10-2019 | 5 | /var/WEB-GUI/cgi- | N/A | O-FIB-HG22- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Limitation of a Pathname to a Restricted Directory ('Path Traversal') | | | bin/downloadfile.cgi on FiberHome HG2201T 1.00.M5007_JS_201804 devices allows pre-authentication Directory Traversal for reading arbitrary files.<br>**CVE ID : CVE-2019-17187** | | 221019/431 |
| **FON** | | | | | |
| **fon2601e-se_firmware** | | | | | |
| Improper Input Validation | 04-10-2019 | 7.8 | FON2601E-SE, FON2601E-RE, FON2601E-FSW-S, and FON2601E-FSW-B with firmware versions 1.1.7 and earlier contain an issue where they may behave as open resolvers. If this vulnerability is exploited, FON routers may be leveraged for DNS amplification attacks to some other entities.<br>**CVE ID : CVE-2019-6015** | N/A | O-FON-FON2-221019/432 |
| **fon2601e-re_firmware** | | | | | |
| Improper Input Validation | 04-10-2019 | 7.8 | FON2601E-SE, FON2601E-RE, FON2601E-FSW-S, and FON2601E-FSW-B with firmware versions 1.1.7 and earlier contain an issue where they may behave as open resolvers. If this vulnerability is exploited, FON routers may be leveraged for DNS amplification attacks to some other entities.<br>**CVE ID : CVE-2019-6015** | N/A | O-FON-FON2-221019/433 |
| **fon2601e-fsw-s_firmware** | | | | | |
| Improper Input | 04-10-2019 | 7.8 | FON2601E-SE, FON2601E-RE, FON2601E-FSW-S, and | N/A | O-FON-FON2- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Validation | | | FON2601E-FSW-B with firmware versions 1.1.7 and earlier contain an issue where they may behave as open resolvers. If this vulnerability is exploited, FON routers may be leveraged for DNS amplification attacks to some other entities.<br>**CVE ID : CVE-2019-6015** | | 221019/434 |
| **fon2601e-fsw-b_firmware** | | | | | |
| Improper Input Validation | 04-10-2019 | 7.8 | FON2601E-SE, FON2601E-RE, FON2601E-FSW-S, and FON2601E-FSW-B with firmware versions 1.1.7 and earlier contain an issue where they may behave as open resolvers. If this vulnerability is exploited, FON routers may be leveraged for DNS amplification attacks to some other entities.<br>**CVE ID : CVE-2019-6015** | N/A | O-FON-FON2-221019/435 |
| **Google** | | | | | |
| **chrome_os** | | | | | |
| Integer Overflow or Wraparound | 01-10-2019 | 9.3 | The Imagination Technologies driver for Chrome OS before R74-11895.B, R75 before R75-12105.B, and R76 before R76-12208.0.0 allows attackers to trigger an Integer Overflow and gain privileges via a malicious application. This occurs because of intentional access for the GPU process to /dev/dri/card1 and the PowerVR ioctl handler, as demonstrated by PVRSRVBridgeSyncPrimOpCre | N/A | O-GOO-CHRO-221019/436 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | ate.<br>**CVE ID : CVE-2019-16508** | | |
| **govicture** | | | | | |
| **pc530_firmware** | | | | | |
| Missing Authentication for Critical Function | 01-10-2019 | 10 | Victure PC530 devices allow unauthenticated TELNET access as root.<br>**CVE ID : CVE-2019-15940** | N/A | O-GOV-PC53-221019/437 |
| **Linux** | | | | | |
| **linux_kernel** | | | | | |
| Incorrect Default Permissions | 01-10-2019 | 2.1 | ax25_create in net/ax25/af_ax25.c in the AF_AX25 network module in the Linux kernel through 5.3.2 does not enforce CAP_NET_RAW, which means that unprivileged users can create a raw socket, aka CID-0614e2b73768.<br>**CVE ID : CVE-2019-17052** | N/A | O-LIN-LINU-221019/438 |
| Incorrect Default Permissions | 01-10-2019 | 2.1 | ieee802154_create in net/ieee802154/socket.c in the AF_IEEE802154 network module in the Linux kernel through 5.3.2 does not enforce CAP_NET_RAW, which means that unprivileged users can create a raw socket, aka CID-e69dbd4619e7.<br>**CVE ID : CVE-2019-17053** | N/A | O-LIN-LINU-221019/439 |
| Incorrect Default Permissions | 01-10-2019 | 2.1 | atalk_create in net/appletalk/ddp.c in the AF_APPLETALK network module in the Linux kernel through 5.3.2 does not enforce CAP_NET_RAW, which means that unprivileged users can | N/A | O-LIN-LINU-221019/440 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | create a raw socket, aka CID-6cc03e8aa36c.<br>**CVE ID : CVE-2019-17054** | | |
| Improper Input Validation | 01-10-2019 | 2.1 | base_sock_create in drivers/isdn/mISDN/socket.c in the AF_ISDN network module in the Linux kernel through 5.3.2 does not enforce CAP_NET_RAW, which means that unprivileged users can create a raw socket, aka CID-b91ee4aa2a21.<br>**CVE ID : CVE-2019-17055** | N/A | O-LIN-LINU-221019/441 |
| Incorrect Default Permissions | 01-10-2019 | 2.1 | llcp_sock_create in net/nfc/llcp_sock.c in the AF_NFC network module in the Linux kernel through 5.3.2 does not enforce CAP_NET_RAW, which means that unprivileged users can create a raw socket, aka CID-3a359798b176.<br>**CVE ID : CVE-2019-17056** | N/A | O-LIN-LINU-221019/442 |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 01-10-2019 | 7.1 | An issue was discovered in write_tpt_entry in drivers/infiniband/hw/cxgb4/mem.c in the Linux kernel through 5.3.2. The cxgb4 driver is directly calling dma_map_single (a DMA function) from a stack variable. This could allow an attacker to trigger a Denial of Service, exploitable if this driver is used on an architecture for which this stack/DMA interaction has security relevance.<br>**CVE ID : CVE-2019-17075** | N/A | O-LIN-LINU-221019/443 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') | 04-10-2019 | 7.5 | In the Linux kernel through 5.3.2, cfg80211_mgd_wext_giwessid in net/wireless/wext-sme.c does not reject a long SSID IE, leading to a Buffer Overflow. **CVE ID : CVE-2019-17133** | N/A | O-LIN-LINU-221019/444 |
| Uncontrolled Resource Consumption | 08-10-2019 | 4.9 | An issue was discovered in drivers/xen/balloon.c in the Linux kernel before 5.2.3, as used in Xen through 4.12.x, allowing guest OS users to cause a denial of service because of unrestricted resource consumption during the mapping of guest memory, aka CID-6ef36ab967c7. **CVE ID : CVE-2019-17351** | N/A | O-LIN-LINU-221019/445 |
| **Microsoft** | | | | | |
| **windows** | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 07-10-2019 | 7.5 | ActiveX Control in MyBuilder before 6.2.2019.814 allow an attacker to execute arbitrary command via the ShellOpen method. This can be leveraged for code execution **CVE ID : CVE-2019-12811** | N/A | O-MIC-WIND-221019/446 |
| Improper Input Validation | 07-10-2019 | 7.5 | MyBuilder viewer before 6.2.2019.814 allow an attacker to execute arbitrary command via specifically crafted configuration file. This can be leveraged for code execution. **CVE ID : CVE-2019-12812** | N/A | O-MIC-WIND-221019/447 |
| Use After Free | 04-10-2019 | 6.8 | This vulnerability allows remote atackers to execute | N/A | O-MIC-WIND- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | arbitrary code on affected installations of Foxit Reader 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the removeField method. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8656.<br>**CVE ID : CVE-2019-13315** | | 221019/448 |
| Use After Free | 04-10-2019 | 6.8 | This vulnerability allows remote atackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Calculate actions. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8757.<br>**CVE ID : CVE-2019-13316** | N/A | O-MIC-WIND-221019/449 |
| Use After | 04-10-2019 | 6.8 | This vulnerability allows | N/A | O-MIC- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Free | | | remote atackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Calculate actions. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8759.<br>**CVE ID : CVE-2019-13317** | | WIND-221019/450 |
| Use of Externally-Controlled Format String | 04-10-2019 | 4.3 | This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Reader 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of the util.printf Javascript method. The application processes the %p parameter in the format string, allowing heap addresses to be returned to the script. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI- | N/A | O-MIC-WIND-221019/451 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | CAN-8544.<br>**CVE ID : CVE-2019-13318** | | |
| Use After Free | 04-10-2019 | 6.8 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of XFA forms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8669.<br>**CVE ID : CVE-2019-13319** | N/A | O-MIC-WIND-221019/452 |
| Use After Free | 04-10-2019 | 6.8 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of AcroForms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current | N/A | O-MIC-WIND-221019/453 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | process. Was ZDI-CAN-8814.<br>**CVE ID : CVE-2019-13320** | | |
| Out-of-bounds Write | 03-10-2019 | 6.8 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Studio Photo 3.6.6.909. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of TIF files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8783.<br>**CVE ID : CVE-2019-13323** | N/A | O-MIC-WIND-221019/454 |
| Out-of-bounds Read | 03-10-2019 | 6.8 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Studio Photo 3.6.6.909. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of TIFF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated | N/A | O-MIC-WIND-221019/455 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8782.<br>**CVE ID : CVE-2019-13324** | | |
| Out-of-bounds Read | 03-10-2019 | 6.8 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Studio Photo 3.6.6.909. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of EPS files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8922.<br>**CVE ID : CVE-2019-13325** | N/A | O-MIC-WIND-221019/456 |
| Out-of-bounds Read | 03-10-2019 | 6.8 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of fields within Acroform objects. The issue | N/A | O-MIC-WIND-221019/457 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8864.<br>**CVE ID : CVE-2019-13326** | | |
| Use After Free | 03-10-2019 | 6.8 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of fields within Acroform objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8888.<br>**CVE ID : CVE-2019-13327** | N/A | O-MIC-WIND-221019/458 |
| Use After Free | 03-10-2019 | 6.8 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the | N/A | O-MIC-WIND-221019/459 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | processing of fields within Acroform objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8913.<br>**CVE ID : CVE-2019-13328** | | |
| Access of Resource Using Incompatible Type ('Type Confusion') | 03-10-2019 | 6.8 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.5. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of TIF files. The issue results from the lack of proper validation of user-supplied data, which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8695.<br>**CVE ID : CVE-2019-13329** | N/A | O-MIC-WIND-221019/460 |
| Access of Resource Using Incompatible Type ('Type Confusion') | 03-10-2019 | 6.8 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The | N/A | O-MIC-WIND-221019/461 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | specific flaw exists within the processing of JPG files. The issue results from the lack of proper validation of user-supplied data, which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8742.<br>**CVE ID : CVE-2019-13330** | | |
| Out-of-bounds Read | 03-10-2019 | 6.8 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JPG files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8838.<br>**CVE ID : CVE-2019-13331** | N/A | O-MIC-WIND-221019/462 |
| Use After Free | 03-10-2019 | 6.8 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.6.0.25114. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or | N/A | O-MIC-WIND-221019/463 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | open a malicious file. The specific flaw exists within the processing of templates in XFA forms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9149.<br>**CVE ID : CVE-2019-13332** | | |
| Allocation of Resources Without Limits or Throttling | 01-10-2019 | 7.5 | PuTTY before 0.73 on Windows improperly opens port-forwarding listening sockets, which allows attackers to listen on the same port to steal an incoming connection.<br>**CVE ID : CVE-2019-17067** | N/A | O-MIC-WIND-221019/464 |
| Missing Release of Resource after Effective Lifetime | 04-10-2019 | 5 | Foxit Reader before 9.7 allows an Access Violation and crash if insufficient memory exists.<br>**CVE ID : CVE-2019-17183** | N/A | O-MIC-WIND-221019/465 |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 05-10-2019 | 5 | www/getfile.php in WPO WebPageTest 19.04 on Windows allows Directory Traversal (for reading arbitrary files) because of an unanchored regular expression, as demonstrated by the a.jpg\.. substring.<br>**CVE ID : CVE-2019-17199** | N/A | O-MIC-WIND-221019/466 |
| Use After Free | 04-10-2019 | 6.8 | This vulnerability allows remote attackers to execute arbitrary code on affected | N/A | O-MIC-WIND-221019/467 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | installations of Foxit Reader 9.4.1.16828. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the deleteItemAt method when processing AcroForms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8295.<br>**CVE ID : CVE-2019-6774** | | |
| Use After Free | 04-10-2019 | 6.8 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the exportValues method within a AcroForm. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8491.<br>**CVE ID : CVE-2019-6775** | N/A | O-MIC-WIND-221019/468 |
| Use After | 04-10-2019 | 6.8 | This vulnerability allows | N/A | O-MIC- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Free | | | remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the removeField method when processing watermarks within AcroForms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-8801.<br>**CVE ID : CVE-2019-6776** | | WIND-221019/469 |
| **windows_10** | | | | | |
| Authentication Bypass by Spoofing | 10-10-2019 | 4.3 | A spoofing vulnerability exists when Microsoft Browsers does not properly parse HTTP content, aka 'Microsoft Browser Spoofing Vulnerability'. This CVE ID is unique from CVE-2019-1357.<br>**CVE ID : CVE-2019-0608** | N/A | O-MIC-WIND-221019/470 |
| Improper Restriction of XML External Entity Reference ('XXE') | 10-10-2019 | 9.3 | A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input, aka 'MS XML Remote Code Execution Vulnerability'.<br>**CVE ID : CVE-2019-1060** | N/A | O-MIC-WIND-221019/471 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 10-10-2019 | 7.1 | A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1239.<br>**CVE ID : CVE-2019-1238** | N/A | O-MIC-WIND-221019/472 |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 10-10-2019 | 7.6 | A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1238.<br>**CVE ID : CVE-2019-1239** | N/A | O-MIC-WIND-221019/473 |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 10-10-2019 | 7.6 | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1308, CVE-2019-1335, CVE-2019-1366.<br>**CVE ID : CVE-2019-1307** | N/A | O-MIC-WIND-221019/474 |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 10-10-2019 | 7.6 | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1307, | N/A | O-MIC-WIND-221019/475 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | CVE-2019-1335, CVE-2019-1366.<br>**CVE ID : CVE-2019-1308** | | |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 10-10-2019 | 9.3 | A remote code execution vulnerability exists when the Windows Imaging API improperly handles objects in memory, aka 'Windows Imaging API Remote Code Execution Vulnerability'.<br>**CVE ID : CVE-2019-1311** | N/A | O-MIC-WIND-221019/476 |
| Improper Privilege Management | 10-10-2019 | 7.2 | An elevation of privilege vulnerability exists when Windows Error Reporting manager improperly handles hard links, aka 'Windows Error Reporting Manager Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1339, CVE-2019-1342.<br>**CVE ID : CVE-2019-1315** | N/A | O-MIC-WIND-221019/477 |
| Improper Privilege Management | 10-10-2019 | 7.2 | An elevation of privilege vulnerability exists in Microsoft Windows Setup when it does not properly handle privileges, aka 'Microsoft Windows Setup Elevation of Privilege Vulnerability'.<br>**CVE ID : CVE-2019-1316** | N/A | O-MIC-WIND-221019/478 |
| Improper Link Resolution Before File Access ('Link Following') | 10-10-2019 | 5.6 | A denial of service vulnerability exists when Windows improperly handles hard links, aka 'Microsoft Windows Denial of Service Vulnerability'.<br>**CVE ID : CVE-2019-1317** | N/A | O-MIC-WIND-221019/479 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Information Exposure | 10-10-2019 | 4.3 | A spoofing vulnerability exists when Transport Layer Security (TLS) accesses non-Extended Master Secret (EMS) sessions, aka 'Microsoft Windows Transport Layer Security Spoofing Vulnerability'. **CVE ID : CVE-2019-1318** | N/A | O-MIC-WIND-221019/480 |
| Improper Privilege Management | 10-10-2019 | 7.2 | An elevation of privilege vulnerability exists in Windows Error Reporting (WER) when WER handles and executes files, aka 'Windows Error Reporting Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1319** | N/A | O-MIC-WIND-221019/481 |
| Improper Authenticati on | 10-10-2019 | 4.6 | An elevation of privilege vulnerability exists when Windows improperly handles authentication requests, aka 'Microsoft Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1322, CVE-2019-1340. **CVE ID : CVE-2019-1320** | N/A | O-MIC-WIND-221019/482 |
| Improper Authenticati on | 10-10-2019 | 4.6 | An elevation of privilege vulnerability exists when Windows improperly handles authentication requests, aka 'Microsoft Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1320, CVE-2019-1340. **CVE ID : CVE-2019-1322** | N/A | O-MIC-WIND-221019/483 |
| Improper Privilege Management | 10-10-2019 | 7.2 | An elevation of privilege vulnerability exists in the Microsoft Windows Update Client when it does not | N/A | O-MIC-WIND-221019/484 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | properly handle privileges, aka 'Microsoft Windows Update Client Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1336.<br>**CVE ID : CVE-2019-1323** | | |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 10-10-2019 | 4.9 | An elevation of privilege vulnerability exists in the Windows redirected drive buffering system (rdbss.sys) when the operating system improperly handles specific local calls within Windows 7 for 32-bit systems, aka 'Windows Redirected Drive Buffering System Elevation of Privilege Vulnerability'.<br>**CVE ID : CVE-2019-1325** | N/A | O-MIC-WIND-221019/485 |
| Improper Input Validation | 10-10-2019 | 7.8 | A denial of service vulnerability exists in Remote Desktop Protocol (RDP) when an attacker connects to the target system using RDP and sends specially crafted requests, aka 'Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability'.<br>**CVE ID : CVE-2019-1326** | N/A | O-MIC-WIND-221019/486 |
| Improper Input Validation | 10-10-2019 | 9.3 | A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server, aka 'Remote Desktop Client Remote Code Execution Vulnerability'.<br>**CVE ID : CVE-2019-1333** | N/A | O-MIC-WIND-221019/487 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 10-10-2019 | 7.6 | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1307, CVE-2019-1308, CVE-2019-1366.<br>**CVE ID : CVE-2019-1335** | N/A | O-MIC-WIND-221019/488 |
| Improper Privilege Management | 10-10-2019 | 7.2 | An elevation of privilege vulnerability exists in the Microsoft Windows Update Client when it does not properly handle privileges, aka 'Microsoft Windows Update Client Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1323.<br>**CVE ID : CVE-2019-1336** | N/A | O-MIC-WIND-221019/489 |
| Information Exposure | 10-10-2019 | 2.1 | An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1334.<br>**CVE ID : CVE-2019-1345** | N/A | O-MIC-WIND-221019/490 |
| Authentication Bypass by Spoofing | 10-10-2019 | 4.3 | A spoofing vulnerability exists when Microsoft Browsers improperly handle browser cookies, aka 'Microsoft Browser Spoofing Vulnerability'. This CVE ID is unique from CVE-2019-0608.<br>**CVE ID : CVE-2019-1357** | N/A | O-MIC-WIND-221019/491 |

| 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 |
|---|---|---|---|---|---|
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 10-10-2019 | 7.6 | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1307, CVE-2019-1308, CVE-2019-1335.<br>**CVE ID : CVE-2019-1366** | N/A | O-MIC-WIND-221019/492 |
| **windows_7** | | | | | |
| Authentication Bypass by Spoofing | 10-10-2019 | 4.3 | A spoofing vulnerability exists when Microsoft Browsers does not properly parse HTTP content, aka 'Microsoft Browser Spoofing Vulnerability'. This CVE ID is unique from CVE-2019-1357.<br>**CVE ID : CVE-2019-0608** | N/A | O-MIC-WIND-221019/493 |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 10-10-2019 | 7.1 | A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1239.<br>**CVE ID : CVE-2019-1238** | N/A | O-MIC-WIND-221019/494 |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 10-10-2019 | 9.3 | A remote code execution vulnerability exists when the Windows Imaging API improperly handles objects in memory, aka 'Windows Imaging API Remote Code Execution Vulnerability'.<br>**CVE ID : CVE-2019-1311** | N/A | O-MIC-WIND-221019/495 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Privilege Management | 10-10-2019 | 7.2 | An elevation of privilege vulnerability exists when Windows Error Reporting manager improperly handles hard links, aka 'Windows Error Reporting Manager Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1339, CVE-2019-1342.<br>**CVE ID : CVE-2019-1315** | N/A | O-MIC-WIND-221019/496 |
| Information Exposure | 10-10-2019 | 4.3 | A spoofing vulnerability exists when Transport Layer Security (TLS) accesses non-Extended Master Secret (EMS) sessions, aka 'Microsoft Windows Transport Layer Security Spoofing Vulnerability'.<br>**CVE ID : CVE-2019-1318** | N/A | O-MIC-WIND-221019/497 |
| Improper Privilege Management | 10-10-2019 | 7.2 | An elevation of privilege vulnerability exists in Windows Error Reporting (WER) when WER handles and executes files, aka 'Windows Error Reporting Elevation of Privilege Vulnerability'.<br>**CVE ID : CVE-2019-1319** | N/A | O-MIC-WIND-221019/498 |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 10-10-2019 | 4.9 | An elevation of privilege vulnerability exists in the Windows redirected drive buffering system (rdbss.sys) when the operating system improperly handles specific local calls within Windows 7 for 32-bit systems, aka 'Windows Redirected Drive Buffering System Elevation of Privilege Vulnerability'. | N/A | O-MIC-WIND-221019/499 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2019-1325** | | |
| Improper Input Validation | 10-10-2019 | 7.8 | A denial of service vulnerability exists in Remote Desktop Protocol (RDP) when an attacker connects to the target system using RDP and sends specially crafted requests, aka 'Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability'.<br>**CVE ID : CVE-2019-1326** | N/A | O-MIC-WIND-221019/500 |
| Improper Input Validation | 10-10-2019 | 9.3 | A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server, aka 'Remote Desktop Client Remote Code Execution Vulnerability'.<br>**CVE ID : CVE-2019-1333** | N/A | O-MIC-WIND-221019/501 |
| Authentication Bypass by Spoofing | 10-10-2019 | 4.3 | A spoofing vulnerability exists when Microsoft Browsers improperly handle browser cookies, aka 'Microsoft Browser Spoofing Vulnerability'. This CVE ID is unique from CVE-2019-0608.<br>**CVE ID : CVE-2019-1357** | N/A | O-MIC-WIND-221019/502 |
| Information Exposure | 10-10-2019 | 4.3 | An information disclosure vulnerability exists in the way that Microsoft Graphics Components handle objects in memory, aka 'Microsoft Graphics Components Information Disclosure Vulnerability'.<br>**CVE ID : CVE-2019-1361** | N/A | O-MIC-WIND-221019/503 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Information Exposure | 10-10-2019 | 2.1 | An information disclosure vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in memory, allowing an attacker to retrieve information from a targeted system, aka 'Windows GDI Information Disclosure Vulnerability'.<br>**CVE ID : CVE-2019-1363** | N/A | O-MIC-WIND-221019/504 |
| **windows_8.1** | | | | | |
| Authentication Bypass by Spoofing | 10-10-2019 | 4.3 | A spoofing vulnerability exists when Microsoft Browsers does not properly parse HTTP content, aka 'Microsoft Browser Spoofing Vulnerability'. This CVE ID is unique from CVE-2019-1357.<br>**CVE ID : CVE-2019-0608** | N/A | O-MIC-WIND-221019/505 |
| Improper Restriction of XML External Entity Reference ('XXE') | 10-10-2019 | 9.3 | A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input, aka 'MS XML Remote Code Execution Vulnerability'.<br>**CVE ID : CVE-2019-1060** | N/A | O-MIC-WIND-221019/506 |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 10-10-2019 | 7.1 | A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1239.<br>**CVE ID : CVE-2019-1238** | N/A | O-MIC-WIND-221019/507 |
| Improper Restriction | 10-10-2019 | 9.3 | A remote code execution vulnerability exists when the | N/A | O-MIC-WIND- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| of Operations within the Bounds of a Memory Buffer | | | Windows Imaging API improperly handles objects in memory, aka 'Windows Imaging API Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-1311** | | 221019/508 |
| Improper Privilege Management | 10-10-2019 | 7.2 | An elevation of privilege vulnerability exists when Windows Error Reporting manager improperly handles hard links, aka 'Windows Error Reporting Manager Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1339, CVE-2019-1342. **CVE ID : CVE-2019-1315** | N/A | O-MIC-WIND-221019/509 |
| Information Exposure | 10-10-2019 | 4.3 | A spoofing vulnerability exists when Transport Layer Security (TLS) accesses non-Extended Master Secret (EMS) sessions, aka 'Microsoft Windows Transport Layer Security Spoofing Vulnerability'. **CVE ID : CVE-2019-1318** | N/A | O-MIC-WIND-221019/510 |
| Improper Privilege Management | 10-10-2019 | 7.2 | An elevation of privilege vulnerability exists in Windows Error Reporting (WER) when WER handles and executes files, aka 'Windows Error Reporting Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1319** | N/A | O-MIC-WIND-221019/511 |
| Improper Restriction of Operations within the | 10-10-2019 | 4.9 | An elevation of privilege vulnerability exists in the Windows redirected drive buffering system (rdbss.sys) when the operating system | N/A | O-MIC-WIND-221019/512 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Bounds of a Memory Buffer | | | improperly handles specific local calls within Windows 7 for 32-bit systems, aka 'Windows Redirected Drive Buffering System Elevation of Privilege Vulnerability'.<br>**CVE ID : CVE-2019-1325** | | |
| Improper Input Validation | 10-10-2019 | 7.8 | A denial of service vulnerability exists in Remote Desktop Protocol (RDP) when an attacker connects to the target system using RDP and sends specially crafted requests, aka 'Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability'.<br>**CVE ID : CVE-2019-1326** | N/A | O-MIC-WIND-221019/513 |
| Improper Input Validation | 10-10-2019 | 9.3 | A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server, aka 'Remote Desktop Client Remote Code Execution Vulnerability'.<br>**CVE ID : CVE-2019-1333** | N/A | O-MIC-WIND-221019/514 |
| Authentication Bypass by Spoofing | 10-10-2019 | 4.3 | A spoofing vulnerability exists when Microsoft Browsers improperly handle browser cookies, aka 'Microsoft Browser Spoofing Vulnerability'. This CVE ID is unique from CVE-2019-0608.<br>**CVE ID : CVE-2019-1357** | N/A | O-MIC-WIND-221019/515 |
| **windows_rt_8.1** | | | | | |
| Authentication Bypass by | 10-10-2019 | 4.3 | A spoofing vulnerability exists when Microsoft Browsers does | N/A | O-MIC-WIND- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Spoofing | | | not properly parse HTTP content, aka 'Microsoft Browser Spoofing Vulnerability'. This CVE ID is unique from CVE-2019-1357.<br>**CVE ID : CVE-2019-0608** | | 221019/516 |
| Improper Restriction of XML External Entity Reference ('XXE') | 10-10-2019 | 9.3 | A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input, aka 'MS XML Remote Code Execution Vulnerability'.<br>**CVE ID : CVE-2019-1060** | N/A | O-MIC-WIND-221019/517 |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 10-10-2019 | 7.1 | A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1239.<br>**CVE ID : CVE-2019-1238** | N/A | O-MIC-WIND-221019/518 |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 10-10-2019 | 9.3 | A remote code execution vulnerability exists when the Windows Imaging API improperly handles objects in memory, aka 'Windows Imaging API Remote Code Execution Vulnerability'.<br>**CVE ID : CVE-2019-1311** | N/A | O-MIC-WIND-221019/519 |
| Improper Privilege Management | 10-10-2019 | 7.2 | An elevation of privilege vulnerability exists when Windows Error Reporting manager improperly handles hard links, aka 'Windows Error Reporting Manager Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1339, | N/A | O-MIC-WIND-221019/520 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | CVE-2019-1342.<br>**CVE ID : CVE-2019-1315** | | |
| Information Exposure | 10-10-2019 | 4.3 | A spoofing vulnerability exists when Transport Layer Security (TLS) accesses non-Extended Master Secret (EMS) sessions, aka 'Microsoft Windows Transport Layer Security Spoofing Vulnerability'.<br>**CVE ID : CVE-2019-1318** | N/A | O-MIC-WIND-221019/521 |
| Improper Privilege Management | 10-10-2019 | 7.2 | An elevation of privilege vulnerability exists in Windows Error Reporting (WER) when WER handles and executes files, aka 'Windows Error Reporting Elevation of Privilege Vulnerability'.<br>**CVE ID : CVE-2019-1319** | N/A | O-MIC-WIND-221019/522 |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 10-10-2019 | 4.9 | An elevation of privilege vulnerability exists in the Windows redirected drive buffering system (rdbss.sys) when the operating system improperly handles specific local calls within Windows 7 for 32-bit systems, aka 'Windows Redirected Drive Buffering System Elevation of Privilege Vulnerability'.<br>**CVE ID : CVE-2019-1325** | N/A | O-MIC-WIND-221019/523 |
| Improper Input Validation | 10-10-2019 | 7.8 | A denial of service vulnerability exists in Remote Desktop Protocol (RDP) when an attacker connects to the target system using RDP and sends specially crafted requests, aka 'Windows Remote Desktop Protocol | N/A | O-MIC-WIND-221019/524 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | (RDP) Denial of Service Vulnerability'.<br>**CVE ID : CVE-2019-1326** | | |
| Improper Input Validation | 10-10-2019 | 9.3 | A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server, aka 'Remote Desktop Client Remote Code Execution Vulnerability'.<br>**CVE ID : CVE-2019-1333** | N/A | O-MIC-WIND-221019/525 |
| Authentication Bypass by Spoofing | 10-10-2019 | 4.3 | A spoofing vulnerability exists when Microsoft Browsers improperly handle browser cookies, aka 'Microsoft Browser Spoofing Vulnerability'. This CVE ID is unique from CVE-2019-0608.<br>**CVE ID : CVE-2019-1357** | N/A | O-MIC-WIND-221019/526 |
| **windows_server_2008** | | | | | |
| Authentication Bypass by Spoofing | 10-10-2019 | 4.3 | A spoofing vulnerability exists when Microsoft Browsers does not properly parse HTTP content, aka 'Microsoft Browser Spoofing Vulnerability'. This CVE ID is unique from CVE-2019-1357.<br>**CVE ID : CVE-2019-0608** | N/A | O-MIC-WIND-221019/527 |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 10-10-2019 | 7.1 | A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1239.<br>**CVE ID : CVE-2019-1238** | N/A | O-MIC-WIND-221019/528 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Privilege Management | 10-10-2019 | 7.2 | An elevation of privilege vulnerability exists when Windows Error Reporting manager improperly handles hard links, aka 'Windows Error Reporting Manager Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1339, CVE-2019-1342.<br>**CVE ID : CVE-2019-1315** | N/A | O-MIC-WIND-221019/529 |
| Information Exposure | 10-10-2019 | 4.3 | A spoofing vulnerability exists when Transport Layer Security (TLS) accesses non-Extended Master Secret (EMS) sessions, aka 'Microsoft Windows Transport Layer Security Spoofing Vulnerability'.<br>**CVE ID : CVE-2019-1318** | N/A | O-MIC-WIND-221019/530 |
| Improper Privilege Management | 10-10-2019 | 7.2 | An elevation of privilege vulnerability exists in Windows Error Reporting (WER) when WER handles and executes files, aka 'Windows Error Reporting Elevation of Privilege Vulnerability'.<br>**CVE ID : CVE-2019-1319** | N/A | O-MIC-WIND-221019/531 |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 10-10-2019 | 4.9 | An elevation of privilege vulnerability exists in the Windows redirected drive buffering system (rdbss.sys) when the operating system improperly handles specific local calls within Windows 7 for 32-bit systems, aka 'Windows Redirected Drive Buffering System Elevation of Privilege Vulnerability'. | N/A | O-MIC-WIND-221019/532 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2019-1325** | | |
| Improper Input Validation | 10-10-2019 | 7.8 | A denial of service vulnerability exists in Remote Desktop Protocol (RDP) when an attacker connects to the target system using RDP and sends specially crafted requests, aka 'Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability'.<br>**CVE ID : CVE-2019-1326** | N/A | O-MIC-WIND-221019/533 |
| Improper Input Validation | 10-10-2019 | 9.3 | A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server, aka 'Remote Desktop Client Remote Code Execution Vulnerability'.<br>**CVE ID : CVE-2019-1333** | N/A | O-MIC-WIND-221019/534 |
| Information Exposure | 10-10-2019 | 4.3 | An information disclosure vulnerability exists in the way that Microsoft Graphics Components handle objects in memory, aka 'Microsoft Graphics Components Information Disclosure Vulnerability'.<br>**CVE ID : CVE-2019-1361** | N/A | O-MIC-WIND-221019/535 |
| Information Exposure | 10-10-2019 | 2.1 | An information disclosure vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in memory, allowing an attacker to retrieve information from a targeted system, aka 'Windows GDI Information Disclosure | N/A | O-MIC-WIND-221019/536 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Vulnerability'.<br>**CVE ID : CVE-2019-1363** | | |
| **windows_server_2012** | | | | | |
| Authentication Bypass by Spoofing | 10-10-2019 | 4.3 | A spoofing vulnerability exists when Microsoft Browsers does not properly parse HTTP content, aka 'Microsoft Browser Spoofing Vulnerability'. This CVE ID is unique from CVE-2019-1357.<br>**CVE ID : CVE-2019-0608** | N/A | O-MIC-WIND-221019/537 |
| Improper Restriction of XML External Entity Reference ('XXE') | 10-10-2019 | 9.3 | A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input, aka 'MS XML Remote Code Execution Vulnerability'.<br>**CVE ID : CVE-2019-1060** | N/A | O-MIC-WIND-221019/538 |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 10-10-2019 | 7.1 | A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1239.<br>**CVE ID : CVE-2019-1238** | N/A | O-MIC-WIND-221019/539 |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 10-10-2019 | 9.3 | A remote code execution vulnerability exists when the Windows Imaging API improperly handles objects in memory, aka 'Windows Imaging API Remote Code Execution Vulnerability'.<br>**CVE ID : CVE-2019-1311** | N/A | O-MIC-WIND-221019/540 |
| Improper Privilege | 10-10-2019 | 7.2 | An elevation of privilege vulnerability exists when Windows Error Reporting | N/A | O-MIC-WIND- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Management | | | manager improperly handles hard links, aka 'Windows Error Reporting Manager Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1339, CVE-2019-1342.<br>**CVE ID : CVE-2019-1315** | | 221019/541 |
| Information Exposure | 10-10-2019 | 4.3 | A spoofing vulnerability exists when Transport Layer Security (TLS) accesses non-Extended Master Secret (EMS) sessions, aka 'Microsoft Windows Transport Layer Security Spoofing Vulnerability'.<br>**CVE ID : CVE-2019-1318** | N/A | O-MIC-WIND-221019/542 |
| Improper Privilege Management | 10-10-2019 | 7.2 | An elevation of privilege vulnerability exists in Windows Error Reporting (WER) when WER handles and executes files, aka 'Windows Error Reporting Elevation of Privilege Vulnerability'.<br>**CVE ID : CVE-2019-1319** | N/A | O-MIC-WIND-221019/543 |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 10-10-2019 | 4.9 | An elevation of privilege vulnerability exists in the Windows redirected drive buffering system (rdbss.sys) when the operating system improperly handles specific local calls within Windows 7 for 32-bit systems, aka 'Windows Redirected Drive Buffering System Elevation of Privilege Vulnerability'.<br>**CVE ID : CVE-2019-1325** | N/A | O-MIC-WIND-221019/544 |
| Improper Input | 10-10-2019 | 7.8 | A denial of service vulnerability exists in Remote | N/A | O-MIC-WIND- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Validation | | | Desktop Protocol (RDP) when an attacker connects to the target system using RDP and sends specially crafted requests, aka 'Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability'.<br>**CVE ID : CVE-2019-1326** | | 221019/545 |
| Improper Input Validation | 10-10-2019 | 9.3 | A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server, aka 'Remote Desktop Client Remote Code Execution Vulnerability'.<br>**CVE ID : CVE-2019-1333** | N/A | O-MIC-WIND-221019/546 |
| Authenticati on Bypass by Spoofing | 10-10-2019 | 4.3 | A spoofing vulnerability exists when Microsoft Browsers improperly handle browser cookies, aka 'Microsoft Browser Spoofing Vulnerability'. This CVE ID is unique from CVE-2019-0608.<br>**CVE ID : CVE-2019-1357** | N/A | O-MIC-WIND-221019/547 |
| **windows_server_2016** | | | | | |
| Authenticati on Bypass by Spoofing | 10-10-2019 | 4.3 | A spoofing vulnerability exists when Microsoft Browsers does not properly parse HTTP content, aka 'Microsoft Browser Spoofing Vulnerability'. This CVE ID is unique from CVE-2019-1357.<br>**CVE ID : CVE-2019-0608** | N/A | O-MIC-WIND-221019/548 |
| Improper Restriction of XML | 10-10-2019 | 9.3 | A remote code execution vulnerability exists when the Microsoft XML Core Services | N/A | O-MIC-WIND-221019/549 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| External Entity Reference ('XXE') | | | MSXML parser processes user input, aka 'MS XML Remote Code Execution Vulnerability'.<br>**CVE ID : CVE-2019-1060** | | |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 10-10-2019 | 7.1 | A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1239.<br>**CVE ID : CVE-2019-1238** | N/A | O-MIC-WIND-221019/550 |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 10-10-2019 | 7.6 | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1308, CVE-2019-1335, CVE-2019-1366.<br>**CVE ID : CVE-2019-1307** | N/A | O-MIC-WIND-221019/551 |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 10-10-2019 | 7.6 | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1307, CVE-2019-1335, CVE-2019-1366.<br>**CVE ID : CVE-2019-1308** | N/A | O-MIC-WIND-221019/552 |
| Improper Restriction | 10-10-2019 | 9.3 | A remote code execution vulnerability exists when the | N/A | O-MIC-WIND- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| of Operations within the Bounds of a Memory Buffer | | | Windows Imaging API improperly handles objects in memory, aka 'Windows Imaging API Remote Code Execution Vulnerability'.<br>**CVE ID : CVE-2019-1311** | | 221019/553 |
| Improper Privilege Management | 10-10-2019 | 7.2 | An elevation of privilege vulnerability exists when Windows Error Reporting manager improperly handles hard links, aka 'Windows Error Reporting Manager Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1339, CVE-2019-1342.<br>**CVE ID : CVE-2019-1315** | N/A | O-MIC-WIND-221019/554 |
| Improper Privilege Management | 10-10-2019 | 7.2 | An elevation of privilege vulnerability exists in Microsoft Windows Setup when it does not properly handle privileges, aka 'Microsoft Windows Setup Elevation of Privilege Vulnerability'.<br>**CVE ID : CVE-2019-1316** | N/A | O-MIC-WIND-221019/555 |
| Improper Link Resolution Before File Access ('Link Following') | 10-10-2019 | 5.6 | A denial of service vulnerability exists when Windows improperly handles hard links, aka 'Microsoft Windows Denial of Service Vulnerability'.<br>**CVE ID : CVE-2019-1317** | N/A | O-MIC-WIND-221019/556 |
| Information Exposure | 10-10-2019 | 4.3 | A spoofing vulnerability exists when Transport Layer Security (TLS) accesses non-Extended Master Secret (EMS) sessions, aka 'Microsoft Windows Transport Layer | N/A | O-MIC-WIND-221019/557 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Security Spoofing Vulnerability'.<br>**CVE ID : CVE-2019-1318** | | |
| Improper Privilege Management | 10-10-2019 | 7.2 | An elevation of privilege vulnerability exists in Windows Error Reporting (WER) when WER handles and executes files, aka 'Windows Error Reporting Elevation of Privilege Vulnerability'.<br>**CVE ID : CVE-2019-1319** | N/A | O-MIC-WIND-221019/558 |
| Improper Authenticati on | 10-10-2019 | 4.6 | An elevation of privilege vulnerability exists when Windows improperly handles authentication requests, aka 'Microsoft Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1322, CVE-2019-1340.<br>**CVE ID : CVE-2019-1320** | N/A | O-MIC-WIND-221019/559 |
| Improper Authenticati on | 10-10-2019 | 4.6 | An elevation of privilege vulnerability exists when Windows improperly handles authentication requests, aka 'Microsoft Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1320, CVE-2019-1340.<br>**CVE ID : CVE-2019-1322** | N/A | O-MIC-WIND-221019/560 |
| Improper Privilege Management | 10-10-2019 | 7.2 | An elevation of privilege vulnerability exists in the Microsoft Windows Update Client when it does not properly handle privileges, aka 'Microsoft Windows Update Client Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1336. | N/A | O-MIC-WIND-221019/561 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2019-1323** | | |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 10-10-2019 | 4.9 | An elevation of privilege vulnerability exists in the Windows redirected drive buffering system (rdbss.sys) when the operating system improperly handles specific local calls within Windows 7 for 32-bit systems, aka 'Windows Redirected Drive Buffering System Elevation of Privilege Vulnerability'.<br>**CVE ID : CVE-2019-1325** | N/A | O-MIC-WIND-221019/562 |
| Improper Input Validation | 10-10-2019 | 7.8 | A denial of service vulnerability exists in Remote Desktop Protocol (RDP) when an attacker connects to the target system using RDP and sends specially crafted requests, aka 'Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability'.<br>**CVE ID : CVE-2019-1326** | N/A | O-MIC-WIND-221019/563 |
| Improper Input Validation | 10-10-2019 | 9.3 | A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server, aka 'Remote Desktop Client Remote Code Execution Vulnerability'.<br>**CVE ID : CVE-2019-1333** | N/A | O-MIC-WIND-221019/564 |
| Improper Restriction of Operations within the Bounds of a | 10-10-2019 | 7.6 | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine | N/A | O-MIC-WIND-221019/565 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Memory Buffer | | | Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1307, CVE-2019-1308, CVE-2019-1366.<br>**CVE ID : CVE-2019-1335** | | |
| Improper Privilege Management | 10-10-2019 | 7.2 | An elevation of privilege vulnerability exists in the Microsoft Windows Update Client when it does not properly handle privileges, aka 'Microsoft Windows Update Client Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1323.<br>**CVE ID : CVE-2019-1336** | N/A | O-MIC-WIND-221019/566 |
| Information Exposure | 10-10-2019 | 2.1 | An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1334.<br>**CVE ID : CVE-2019-1345** | N/A | O-MIC-WIND-221019/567 |
| Authentication Bypass by Spoofing | 10-10-2019 | 4.3 | A spoofing vulnerability exists when Microsoft Browsers improperly handle browser cookies, aka 'Microsoft Browser Spoofing Vulnerability'. This CVE ID is unique from CVE-2019-0608.<br>**CVE ID : CVE-2019-1357** | N/A | O-MIC-WIND-221019/568 |
| Improper Restriction of Operations within the Bounds of a | 10-10-2019 | 7.6 | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine | N/A | O-MIC-WIND-221019/569 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Memory Buffer | | | Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1307, CVE-2019-1308, CVE-2019-1335.<br>**CVE ID : CVE-2019-1366** | | |
| **windows_server_2019** | | | | | |
| Authentication Bypass by Spoofing | 10-10-2019 | 4.3 | A spoofing vulnerability exists when Microsoft Browsers does not properly parse HTTP content, aka 'Microsoft Browser Spoofing Vulnerability'. This CVE ID is unique from CVE-2019-1357.<br>**CVE ID : CVE-2019-0608** | N/A | O-MIC-WIND-221019/570 |
| Improper Restriction of XML External Entity Reference ('XXE') | 10-10-2019 | 9.3 | A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input, aka 'MS XML Remote Code Execution Vulnerability'.<br>**CVE ID : CVE-2019-1060** | N/A | O-MIC-WIND-221019/571 |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 10-10-2019 | 7.1 | A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1239.<br>**CVE ID : CVE-2019-1238** | N/A | O-MIC-WIND-221019/572 |
| Improper Restriction of Operations within the Bounds of a Memory | 10-10-2019 | 7.6 | A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE- | N/A | O-MIC-WIND-221019/573 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Buffer | | | 2019-1238.<br>**CVE ID : CVE-2019-1239** | | |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 10-10-2019 | 7.6 | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1308, CVE-2019-1335, CVE-2019-1366.<br>**CVE ID : CVE-2019-1307** | N/A | O-MIC-WIND-221019/574 |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 10-10-2019 | 7.6 | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1307, CVE-2019-1335, CVE-2019-1366.<br>**CVE ID : CVE-2019-1308** | N/A | O-MIC-WIND-221019/575 |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 10-10-2019 | 9.3 | A remote code execution vulnerability exists when the Windows Imaging API improperly handles objects in memory, aka 'Windows Imaging API Remote Code Execution Vulnerability'.<br>**CVE ID : CVE-2019-1311** | N/A | O-MIC-WIND-221019/576 |
| Improper Privilege Management | 10-10-2019 | 7.2 | An elevation of privilege vulnerability exists when Windows Error Reporting manager improperly handles hard links, aka 'Windows | N/A | O-MIC-WIND-221019/577 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Error Reporting Manager Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1339, CVE-2019-1342.<br>**CVE ID : CVE-2019-1315** | | |
| Improper Privilege Management | 10-10-2019 | 7.2 | An elevation of privilege vulnerability exists in Microsoft Windows Setup when it does not properly handle privileges, aka 'Microsoft Windows Setup Elevation of Privilege Vulnerability'.<br>**CVE ID : CVE-2019-1316** | N/A | O-MIC-WIND-221019/578 |
| Improper Link Resolution Before File Access ('Link Following') | 10-10-2019 | 5.6 | A denial of service vulnerability exists when Windows improperly handles hard links, aka 'Microsoft Windows Denial of Service Vulnerability'.<br>**CVE ID : CVE-2019-1317** | N/A | O-MIC-WIND-221019/579 |
| Information Exposure | 10-10-2019 | 4.3 | A spoofing vulnerability exists when Transport Layer Security (TLS) accesses non-Extended Master Secret (EMS) sessions, aka 'Microsoft Windows Transport Layer Security Spoofing Vulnerability'.<br>**CVE ID : CVE-2019-1318** | N/A | O-MIC-WIND-221019/580 |
| Improper Privilege Management | 10-10-2019 | 7.2 | An elevation of privilege vulnerability exists in Windows Error Reporting (WER) when WER handles and executes files, aka 'Windows Error Reporting Elevation of Privilege Vulnerability'. | N/A | O-MIC-WIND-221019/581 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2019-1319** | | |
| Improper Authentication | 10-10-2019 | 4.6 | An elevation of privilege vulnerability exists when Windows improperly handles authentication requests, aka 'Microsoft Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1322, CVE-2019-1340.<br>**CVE ID : CVE-2019-1320** | N/A | O-MIC-WIND-221019/582 |
| Improper Authentication | 10-10-2019 | 4.6 | An elevation of privilege vulnerability exists when Windows improperly handles authentication requests, aka 'Microsoft Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1320, CVE-2019-1340.<br>**CVE ID : CVE-2019-1322** | N/A | O-MIC-WIND-221019/583 |
| Improper Privilege Management | 10-10-2019 | 7.2 | An elevation of privilege vulnerability exists in the Microsoft Windows Update Client when it does not properly handle privileges, aka 'Microsoft Windows Update Client Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1336.<br>**CVE ID : CVE-2019-1323** | N/A | O-MIC-WIND-221019/584 |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 10-10-2019 | 4.9 | An elevation of privilege vulnerability exists in the Windows redirected drive buffering system (rdbss.sys) when the operating system improperly handles specific local calls within Windows 7 for 32-bit systems, aka 'Windows Redirected Drive Buffering System Elevation of | N/A | O-MIC-WIND-221019/585 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Privilege Vulnerability'.<br>**CVE ID : CVE-2019-1325** | | |
| Improper Input Validation | 10-10-2019 | 7.8 | A denial of service vulnerability exists in Remote Desktop Protocol (RDP) when an attacker connects to the target system using RDP and sends specially crafted requests, aka 'Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability'.<br>**CVE ID : CVE-2019-1326** | N/A | O-MIC-WIND-221019/586 |
| Improper Input Validation | 10-10-2019 | 9.3 | A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server, aka 'Remote Desktop Client Remote Code Execution Vulnerability'.<br>**CVE ID : CVE-2019-1333** | N/A | O-MIC-WIND-221019/587 |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 10-10-2019 | 7.6 | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1307, CVE-2019-1308, CVE-2019-1366.<br>**CVE ID : CVE-2019-1335** | N/A | O-MIC-WIND-221019/588 |
| Improper Privilege Management | 10-10-2019 | 7.2 | An elevation of privilege vulnerability exists in the Microsoft Windows Update Client when it does not properly handle privileges, aka | N/A | O-MIC-WIND-221019/589 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | 'Microsoft Windows Update Client Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1323.<br>**CVE ID : CVE-2019-1336** | | |
| Information Exposure | 10-10-2019 | 2.1 | An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1334.<br>**CVE ID : CVE-2019-1345** | N/A | O-MIC-WIND-221019/590 |
| Authentication Bypass by Spoofing | 10-10-2019 | 4.3 | A spoofing vulnerability exists when Microsoft Browsers improperly handle browser cookies, aka 'Microsoft Browser Spoofing Vulnerability'. This CVE ID is unique from CVE-2019-0608.<br>**CVE ID : CVE-2019-1357** | N/A | O-MIC-WIND-221019/591 |
| Improper Restriction of Operations within the Bounds of a Memory Buffer | 10-10-2019 | 7.6 | A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1307, CVE-2019-1308, CVE-2019-1335.<br>**CVE ID : CVE-2019-1366** | N/A | O-MIC-WIND-221019/592 |
| **nixos** | | | | | |
| **nix** | | | | | |
| Incorrect Default | 09-10-2019 | 4.6 | Nix through 2.3 allows local users to gain access to an | N/A | O-NIX-NIX-221019/593 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Permissions | | | arbitrary user's account because the parent directory of the user-profile directories is world writable.<br>**CVE ID : CVE-2019-17365** | | |
| **opengroup** | | | | | |
| **unix** | | | | | |
| Insufficient Verification of Data Authenticity | 03-10-2019 | 5 | rpcapd/daemon.c in libpcap before 1.9.1 on non-Windows platforms provides details about why authentication failed, which might make it easier for attackers to enumerate valid usernames.<br>**CVE ID : CVE-2019-15162** | https://github.com/the-tcpdump-group/libpcap/blob/libpcap-1.9/CHANGES, https://github.com/the-tcpdump-group/libpcap/commit/484d60cbf7ca4ec758c3cbb8a82d68b244a78d58, https://www.tcpdump.org/public-cve-list.txt | O-OPE-UNIX-221019/594 |
| **Opensuse** | | | | | |
| **leap** | | | | | |
| Improper Neutralization of Special Elements in Output Used | 01-10-2019 | 5 | PuTTY before 0.73 mishandles the "bracketed paste mode" protection mechanism, which may allow a session to be affected by malicious | N/A | O-OPE-LEAP-221019/595 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| by a Downstream Component ('Injection') | | | clipboard content.<br>**CVE ID : CVE-2019-17068** | | |
| Improper Input Validation | 01-10-2019 | 5 | PuTTY before 0.73 might allow remote SSH-1 servers to cause a denial of service by accessing freed memory locations via an SSH1_MSG_DISCONNECT message.<br>**CVE ID : CVE-2019-17069** | N/A | O-OPE-LEAP-221019/596 |
| **Redhat** | | | | | |
| **enterprise_linux** | | | | | |
| Deserialization of Untrusted Data | 01-10-2019 | 7.5 | A series of deserialization vulnerabilities have been discovered in Codehaus 1.9.x implemented in EAP 7. This CVE fixes CVE-2017-17485, CVE-2017-7525, CVE-2017-15095, CVE-2018-5968, CVE-2018-7489, CVE-2018-1000873, CVE-2019-12086 reported for FasterXML jackson-databind by implementing a whitelist approach that will mitigate these vulnerabilities and future ones alike.<br>**CVE ID : CVE-2019-10202** | https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-10202 | O-RED-ENTE-221019/597 |
| **socomec** | | | | | |
| **diris_a-40_firmware** | | | | | |
| Insufficiently Protected Credentials | 09-10-2019 | 10 | Password disclosure in the web interface on socomec DIRIS A-40 devices before 48250501 allows a remote attacker to get full access to a device via the /password.jsn URI. | N/A | O-SOC-DIRI-221019/598 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2019-15859** | | |
| **Suse** | | | | | |
| **suse_linux_enterprise_server** | | | | | |
| Incorrect Default Permissions | 07-10-2019 | 6.6 | The /usr/sbin/pinger binary packaged with squid in SUSE Linux Enterprise Server 15 before and including version 4.8-5.8.1 and in SUSE Linux Enterprise Server 12 before and including 3.5.21-26.17.1 had squid:root, 0750 permissions. This allowed an attacker that compromissed the squid user to gain persistence by changing the binary<br>**CVE ID : CVE-2019-3688** | https://bugzilla.suse.com/show_bug.cgi?id=1093414 | O-SUS-SUSE-221019/599 |
| **vzug** | | | | | |
| **combi-stream_mslq_firmware** | | | | | |
| Improper Authentication | 06-10-2019 | 5 | An issue was discovered on V-Zug Combi-Steam MSLQ devices before Ethernet R07 and before WLAN R05. There is no bruteforce protection (e.g., lockout) established. An attacker might be able to bruteforce the password to authenticate on the device.<br>**CVE ID : CVE-2019-17215** | N/A | O-VZU-COMB-221019/600 |
| Improper Authentication | 06-10-2019 | 7.5 | An issue was discovered on V-Zug Combi-Steam MSLQ devices before Ethernet R07 and before WLAN R05. Password authentication uses MD5 to hash passwords. Cracking is possible with minimal effort.<br>**CVE ID : CVE-2019-17216** | N/A | O-VZU-COMB-221019/601 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Cross-Site Request Forgery (CSRF) | 06-10-2019 | 6.8 | An issue was discovered on V-Zug Combi-Steam MSLQ devices before Ethernet R07 and before WLAN R05. There is no CSRF protection established on the web service.<br>**CVE ID : CVE-2019-17217** | N/A | O-VZU-COMB-221019/602 |
| Missing Encryption of Sensitive Data | 06-10-2019 | 5 | An issue was discovered on V-Zug Combi-Steam MSLQ devices before Ethernet R07 and before WLAN R05. By default, the communication to the web service is unencrypted via http. An attacker is able to intercept and sniff communication to the web service.<br>**CVE ID : CVE-2019-17218** | N/A | O-VZU-COMB-221019/603 |
| Improper Authenticati on | 06-10-2019 | 5.8 | An issue was discovered on V-Zug Combi-Steam MSLQ devices before Ethernet R07 and before WLAN R05. By default, the device does not enforce any authentication. An adjacent attacker is able to use the network interface without proper access control.<br>**CVE ID : CVE-2019-17219** | N/A | O-VZU-COMB-221019/604 |
| **XEN** | | | | | |
| **xen** | | | | | |
| Improper Input Validation | 08-10-2019 | 6.1 | An issue was discovered in Xen through 4.11.x allowing x86 guest OS users to cause a denial of service or gain privileges because grant-table transfer requests are mishandled.<br>**CVE ID : CVE-2019-17340** | N/A | O-XEN-XEN-221019/605 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 08-10-2019 | 6.9 | An issue was discovered in Xen through 4.11.x allowing x86 PV guest OS users to cause a denial of service or gain privileges by leveraging a page-writability race condition during addition of a passed-through PCI device.<br>**CVE ID : CVE-2019-17341** | N/A | O-XEN-XEN-221019/606 |
| Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 08-10-2019 | 4.4 | An issue was discovered in Xen through 4.11.x allowing x86 PV guest OS users to cause a denial of service or gain privileges by leveraging a race condition that arose when XENMEM_exchange was introduced.<br>**CVE ID : CVE-2019-17342** | N/A | O-XEN-XEN-221019/607 |
| Improper Input Validation | 08-10-2019 | 4.6 | An issue was discovered in Xen through 4.11.x allowing x86 PV guest OS users to cause a denial of service or gain privileges by leveraging incorrect use of the HVM physmap concept for PV domains.<br>**CVE ID : CVE-2019-17343** | N/A | O-XEN-XEN-221019/608 |
| Improper Input Validation | 08-10-2019 | 4.9 | An issue was discovered in Xen through 4.11.x allowing x86 PV guest OS users to cause a denial of service by leveraging a long-running operation that exists to support restartability of PTE updates.<br>**CVE ID : CVE-2019-17344** | N/A | O-XEN-XEN-221019/609 |
| Improper Input | 08-10-2019 | 4.9 | An issue was discovered in Xen 4.8.x through 4.11.x allowing x86 PV guest OS | N/A | O-XEN-XEN-221019/610 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Validation | | | users to cause a denial of service because mishandling of failed IOMMU operations causes a bug check during the cleanup of a crashed guest.<br>**CVE ID : CVE-2019-17345** | | |
| Improper Input Validation | 08-10-2019 | 7.2 | An issue was discovered in Xen through 4.11.x allowing x86 PV guest OS users to cause a denial of service or gain privileges because of an incompatibility between Process Context Identifiers (PCID) and TLB flushes.<br>**CVE ID : CVE-2019-17346** | N/A | O-XEN-XEN-221019/611 |
| Improper Input Validation | 08-10-2019 | 4.6 | An issue was discovered in Xen through 4.11.x allowing x86 PV guest OS users to cause a denial of service or gain privileges because a guest can manipulate its virtualised %cr4 in a way that is incompatible with Linux (and possibly other guest kernels).<br>**CVE ID : CVE-2019-17347** | N/A | O-XEN-XEN-221019/612 |
| Improper Input Validation | 08-10-2019 | 4.9 | An issue was discovered in Xen through 4.11.x allowing x86 PV guest OS users to cause a denial of service because of an incompatibility between Process Context Identifiers (PCID) and shadow-pagetable switching.<br>**CVE ID : CVE-2019-17348** | N/A | O-XEN-XEN-221019/613 |
| Loop with Unreachable Exit Condition ('Infinite | 08-10-2019 | 4.9 | An issue was discovered in Xen through 4.12.x allowing Arm domU attackers to cause a denial of service (infinite loop) involving a LoadExcl or | N/A | O-XEN-XEN-221019/614 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Loop') | | | StoreExcl operation.<br>**CVE ID : CVE-2019-17349** | | |
| Loop with Unreachable Exit Condition ('Infinite Loop') | 08-10-2019 | 4.9 | An issue was discovered in Xen through 4.12.x allowing Arm domU attackers to cause a denial of service (infinite loop) involving a compare-and-exchange operation.<br>**CVE ID : CVE-2019-17350** | N/A | O-XEN-XEN-221019/615 |
| Uncontrolled Resource Consumption | 08-10-2019 | 4.9 | An issue was discovered in drivers/xen/balloon.c in the Linux kernel before 5.2.3, as used in Xen through 4.12.x, allowing guest OS users to cause a denial of service because of unrestricted resource consumption during the mapping of guest memory, aka CID-6ef36ab967c7.<br>**CVE ID : CVE-2019-17351** | N/A | O-XEN-XEN-221019/616 |
| **Xerox** | | | | | |
| **atlalink_firmware** | | | | | |
| Improper Privilege Management | 04-10-2019 | 7.5 | Xerox AtlaLink B8045/B8055/B8065/B8075/ B8090 C8030/C8035/C8045/C8055/ C8070 printers with software before 101.00x.089.22600 allow an attacker to gain privileges.<br>**CVE ID : CVE-2019-17184** | N/A | O-XER-ATLA-221019/617 |
| **Hardware** | | | | | |
| **Cisco** | | | | | |
| **asa_5505** | | | | | |
| Improper Input Validation | 02-10-2019 | 5 | A vulnerability in the FTP inspection engine of Cisco Adaptive Security (ASA) | N/A | H-CIS-ASA_-221019/618 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of FTP data. An attacker could exploit this vulnerability by sending malicious FTP traffic through an affected device. A successful exploit could allow the attacker to cause a DoS condition on the affected device.<br>**CVE ID : CVE-2019-12673** | | |
| Improper Input Validation | 02-10-2019 | 3.3 | A vulnerability in the Open Shortest Path First (OSPF) implementation of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability exists because the affected software improperly parses certain options in OSPF link-state advertisement (LSA) type 11 packets. An attacker could exploit this vulnerability by sending a crafted LSA type 11 OSPF packet to an affected device. A successful exploit could allow the attacker to cause a reload of the affected | N/A | H-CIS-ASA_-221019/619 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | device, resulting in a DoS condition for client traffic that is traversing the device.<br>**CVE ID : CVE-2019-12676** | | |
| Improper Handling of Exceptional Conditions | 02-10-2019 | 4 | A vulnerability in the Secure Sockets Layer (SSL) VPN feature of Cisco Adaptive Security Appliance (ASA) Software could allow an authenticated, remote attacker to cause a denial of service (DoS) condition that prevents the creation of new SSL/Transport Layer Security (TLS) connections to an affected device. The vulnerability is due to incorrect handling of Base64-encoded strings. An attacker could exploit this vulnerability by opening many SSL VPN sessions to an affected device. The attacker would need to have valid user credentials on the affected device to exploit this vulnerability. A successful exploit could allow the attacker to overwrite a special system memory location, which will eventually result in memory allocation errors for new SSL/TLS sessions to the device, preventing successful establishment of these sessions. A reload of the device is required to recover from this condition. Established SSL/TLS connections to the device and SSL/TLS connections through the device are not affected. Note: | N/A | H-CIS-ASA_-221019/620 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Although this vulnerability is in the SSL VPN feature, successful exploitation of this vulnerability would affect all new SSL/TLS sessions to the device, including management sessions.<br>**CVE ID : CVE-2019-12677** | | |
| Integer Underflow (Wrap or Wraparound) | 02-10-2019 | 5 | A vulnerability in the Session Initiation Protocol (SIP) inspection module of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper parsing of SIP messages. An attacker could exploit this vulnerability by sending a malicious SIP packet through an affected device. A successful exploit could allow the attacker to trigger an integer underflow, causing the software to try to read unmapped memory and resulting in a crash.<br>**CVE ID : CVE-2019-12678** | N/A | H-CIS-ASA_-221019/621 |
| Incorrect Type Conversion or Cast | 02-10-2019 | 4 | A vulnerability in the Secure Copy (SCP) feature of Cisco Adaptive Security Appliance (ASA) Software could allow an authenticated, remote attacker to cause a denial of service (DoS) condition. The vulnerability is due to the use | N/A | H-CIS-ASA_-221019/622 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | of an incorrect data type for a length variable. An attacker could exploit this vulnerability by initiating the transfer of a large file to an affected device via SCP. To exploit this vulnerability, the attacker would need to have valid privilege level 15 credentials on the affected device. A successful exploit could allow the attacker to cause the length variable to roll over, which could cause the affected device to crash.<br>**CVE ID : CVE-2019-12693** | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 02-10-2019 | 4.3 | A vulnerability in the Clientless SSL VPN (WebVPN) portal of Cisco Adaptive Security Appliance (ASA) and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or allow the | N/A | H-CIS-ASA_-221019/623 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | attacker to access sensitive browser-based information.<br>**CVE ID : CVE-2019-12695** | | |
| Uncontrolled Resource Consumption | 02-10-2019 | 7.8 | A vulnerability in the WebVPN feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause increased CPU utilization on an affected device. The vulnerability is due to excessive processing load for a specific WebVPN HTTP page request. An attacker could exploit this vulnerability by sending multiple WebVPN HTTP page load requests for a specific URL. A successful exploit could allow the attacker to increase CPU load on the device, resulting in a denial of service (DoS) condition, which could cause traffic to be delayed through the device.<br>**CVE ID : CVE-2019-12698** | N/A | H-CIS-ASA_-221019/624 |
| Uncontrolled Resource Consumption | 02-10-2019 | 7.8 | A vulnerability in the Internet Key Exchange version 1 (IKEv1) feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is | N/A | H-CIS-ASA_-221019/625 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | due to improper management of system memory. An attacker could exploit this vulnerability by sending malicious IKEv1 traffic to an affected device. The attacker does not need valid credentials to authenticate the VPN session, nor does the attacker's source address need to match a peer statement in the crypto map applied to the ingress interface of the affected device. An exploit could allow the attacker to exhaust system memory resources, leading to a reload of an affected device.<br>**CVE ID : CVE-2019-15256** | | |
| **asa_5510** | | | | | |
| Improper Input Validation | 02-10-2019 | 5 | A vulnerability in the FTP inspection engine of Cisco Adaptive Security (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of FTP data. An attacker could exploit this vulnerability by sending malicious FTP traffic through an affected device. A successful exploit could allow the attacker to cause a DoS condition on the affected device.<br>**CVE ID : CVE-2019-12673** | N/A | H-CIS-ASA_-221019/626 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Input Validation | 02-10-2019 | 3.3 | A vulnerability in the Open Shortest Path First (OSPF) implementation of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability exists because the affected software improperly parses certain options in OSPF link-state advertisement (LSA) type 11 packets. An attacker could exploit this vulnerability by sending a crafted LSA type 11 OSPF packet to an affected device. A successful exploit could allow the attacker to cause a reload of the affected device, resulting in a DoS condition for client traffic that is traversing the device.<br>**CVE ID : CVE-2019-12676** | N/A | H-CIS-ASA_-221019/627 |
| Improper Handling of Exceptional Conditions | 02-10-2019 | 4 | A vulnerability in the Secure Sockets Layer (SSL) VPN feature of Cisco Adaptive Security Appliance (ASA) Software could allow an authenticated, remote attacker to cause a denial of service (DoS) condition that prevents the creation of new SSL/Transport Layer Security (TLS) connections to an affected device. The vulnerability is due to incorrect handling of Base64- | N/A | H-CIS-ASA_-221019/628 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | encoded strings. An attacker could exploit this vulnerability by opening many SSL VPN sessions to an affected device. The attacker would need to have valid user credentials on the affected device to exploit this vulnerability. A successful exploit could allow the attacker to overwrite a special system memory location, which will eventually result in memory allocation errors for new SSL/TLS sessions to the device, preventing successful establishment of these sessions. A reload of the device is required to recover from this condition. Established SSL/TLS connections to the device and SSL/TLS connections through the device are not affected. Note: Although this vulnerability is in the SSL VPN feature, successful exploitation of this vulnerability would affect all new SSL/TLS sessions to the device, including management sessions.<br>**CVE ID : CVE-2019-12677** | | |
| Integer Underflow (Wrap or Wraparound ) | 02-10-2019 | 5 | A vulnerability in the Session Initiation Protocol (SIP) inspection module of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an | N/A | H-CIS-ASA_-221019/629 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | affected device. The vulnerability is due to improper parsing of SIP messages. An attacker could exploit this vulnerability by sending a malicious SIP packet through an affected device. A successful exploit could allow the attacker to trigger an integer underflow, causing the software to try to read unmapped memory and resulting in a crash.<br>**CVE ID : CVE-2019-12678** | | |
| Incorrect Type Conversion or Cast | 02-10-2019 | 4 | A vulnerability in the Secure Copy (SCP) feature of Cisco Adaptive Security Appliance (ASA) Software could allow an authenticated, remote attacker to cause a denial of service (DoS) condition. The vulnerability is due to the use of an incorrect data type for a length variable. An attacker could exploit this vulnerability by initiating the transfer of a large file to an affected device via SCP. To exploit this vulnerability, the attacker would need to have valid privilege level 15 credentials on the affected device. A successful exploit could allow the attacker to cause the length variable to roll over, which could cause the affected device to crash.<br>**CVE ID : CVE-2019-12693** | N/A | H-CIS-ASA_-221019/630 |
| Improper Neutralizatio | 02-10-2019 | 4.3 | A vulnerability in the Clientless SSL VPN (WebVPN) | N/A | H-CIS-ASA_-221019/631 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| n of Input During Web Page Generation ('Cross-site Scripting') | | | portal of Cisco Adaptive Security Appliance (ASA) and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or allow the attacker to access sensitive browser-based information.<br>**CVE ID : CVE-2019-12695** | | |
| Uncontrolled Resource Consumption | 02-10-2019 | 7.8 | A vulnerability in the WebVPN feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause increased CPU utilization on an affected device. The vulnerability is due to excessive processing load for a specific WebVPN HTTP page request. An attacker could exploit this vulnerability by sending multiple WebVPN | N/A | H-CIS-ASA_-221019/632 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | HTTP page load requests for a specific URL. A successful exploit could allow the attacker to increase CPU load on the device, resulting in a denial of service (DoS) condition, which could cause traffic to be delayed through the device.<br>**CVE ID : CVE-2019-12698** | | |
| Uncontrolled Resource Consumption | 02-10-2019 | 7.8 | A vulnerability in the Internet Key Exchange version 1 (IKEv1) feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to improper management of system memory. An attacker could exploit this vulnerability by sending malicious IKEv1 traffic to an affected device. The attacker does not need valid credentials to authenticate the VPN session, nor does the attacker's source address need to match a peer statement in the crypto map applied to the ingress interface of the affected device. An exploit could allow the attacker to exhaust system memory resources, leading to a reload of an affected device.<br>**CVE ID : CVE-2019-15256** | N/A | H-CIS-ASA_-221019/633 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **asa_5512-x** | | | | | |
| Improper Input Validation | 02-10-2019 | 5 | A vulnerability in the FTP inspection engine of Cisco Adaptive Security (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of FTP data. An attacker could exploit this vulnerability by sending malicious FTP traffic through an affected device. A successful exploit could allow the attacker to cause a DoS condition on the affected device.<br>**CVE ID : CVE-2019-12673** | N/A | H-CIS-ASA_-221019/634 |
| Improper Input Validation | 02-10-2019 | 3.3 | A vulnerability in the Open Shortest Path First (OSPF) implementation of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability exists because the affected software improperly parses certain options in OSPF link-state advertisement (LSA) type 11 packets. An attacker could exploit this vulnerability by | N/A | H-CIS-ASA_-221019/635 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | sending a crafted LSA type 11 OSPF packet to an affected device. A successful exploit could allow the attacker to cause a reload of the affected device, resulting in a DoS condition for client traffic that is traversing the device.<br>**CVE ID : CVE-2019-12676** | | |
| Improper Handling of Exceptional Conditions | 02-10-2019 | 4 | A vulnerability in the Secure Sockets Layer (SSL) VPN feature of Cisco Adaptive Security Appliance (ASA) Software could allow an authenticated, remote attacker to cause a denial of service (DoS) condition that prevents the creation of new SSL/Transport Layer Security (TLS) connections to an affected device. The vulnerability is due to incorrect handling of Base64-encoded strings. An attacker could exploit this vulnerability by opening many SSL VPN sessions to an affected device. The attacker would need to have valid user credentials on the affected device to exploit this vulnerability. A successful exploit could allow the attacker to overwrite a special system memory location, which will eventually result in memory allocation errors for new SSL/TLS sessions to the device, preventing successful establishment of these sessions. A reload of the device is required to recover from | N/A | H-CIS-ASA_-221019/636 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | this condition. Established SSL/TLS connections to the device and SSL/TLS connections through the device are not affected. Note: Although this vulnerability is in the SSL VPN feature, successful exploitation of this vulnerability would affect all new SSL/TLS sessions to the device, including management sessions.<br>**CVE ID : CVE-2019-12677** | | |
| Integer Underflow (Wrap or Wraparound) | 02-10-2019 | 5 | A vulnerability in the Session Initiation Protocol (SIP) inspection module of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper parsing of SIP messages. An attacker could exploit this vulnerability by sending a malicious SIP packet through an affected device. A successful exploit could allow the attacker to trigger an integer underflow, causing the software to try to read unmapped memory and resulting in a crash.<br>**CVE ID : CVE-2019-12678** | N/A | H-CIS-ASA_-221019/637 |
| Incorrect Type Conversion | 02-10-2019 | 4 | A vulnerability in the Secure Copy (SCP) feature of Cisco Adaptive Security Appliance | N/A | H-CIS-ASA_-221019/638 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| or Cast | | | (ASA) Software could allow an authenticated, remote attacker to cause a denial of service (DoS) condition. The vulnerability is due to the use of an incorrect data type for a length variable. An attacker could exploit this vulnerability by initiating the transfer of a large file to an affected device via SCP. To exploit this vulnerability, the attacker would need to have valid privilege level 15 credentials on the affected device. A successful exploit could allow the attacker to cause the length variable to roll over, which could cause the affected device to crash.<br>**CVE ID : CVE-2019-12693** | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 02-10-2019 | 4.3 | A vulnerability in the Clientless SSL VPN (WebVPN) portal of Cisco Adaptive Security Appliance (ASA) and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a | N/A | H-CIS-ASA_-221019/639 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or allow the attacker to access sensitive browser-based information.<br>**CVE ID : CVE-2019-12695** | | |
| Uncontrolled Resource Consumption | 02-10-2019 | 7.8 | A vulnerability in the WebVPN feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause increased CPU utilization on an affected device. The vulnerability is due to excessive processing load for a specific WebVPN HTTP page request. An attacker could exploit this vulnerability by sending multiple WebVPN HTTP page load requests for a specific URL. A successful exploit could allow the attacker to increase CPU load on the device, resulting in a denial of service (DoS) condition, which could cause traffic to be delayed through the device.<br>**CVE ID : CVE-2019-12698** | N/A | H-CIS-ASA_-221019/640 |
| Uncontrolled Resource Consumption | 02-10-2019 | 7.8 | A vulnerability in the Internet Key Exchange version 1 (IKEv1) feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an | N/A | H-CIS-ASA_-221019/641 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | unauthenticated, remote attacker to trigger a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to improper management of system memory. An attacker could exploit this vulnerability by sending malicious IKEv1 traffic to an affected device. The attacker does not need valid credentials to authenticate the VPN session, nor does the attacker's source address need to match a peer statement in the crypto map applied to the ingress interface of the affected device. An exploit could allow the attacker to exhaust system memory resources, leading to a reload of an affected device.<br>**CVE ID : CVE-2019-15256** | | |
| **asa_5515-x** | | | | | |
| Improper Input Validation | 02-10-2019 | 5 | A vulnerability in the FTP inspection engine of Cisco Adaptive Security (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of FTP data. An attacker could exploit this vulnerability by sending malicious FTP traffic through an affected device. A successful | N/A | H-CIS-ASA_-221019/642 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | exploit could allow the attacker to cause a DoS condition on the affected device.<br>**CVE ID : CVE-2019-12673** | | |
| Improper Input Validation | 02-10-2019 | 3.3 | A vulnerability in the Open Shortest Path First (OSPF) implementation of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability exists because the affected software improperly parses certain options in OSPF link-state advertisement (LSA) type 11 packets. An attacker could exploit this vulnerability by sending a crafted LSA type 11 OSPF packet to an affected device. A successful exploit could allow the attacker to cause a reload of the affected device, resulting in a DoS condition for client traffic that is traversing the device.<br>**CVE ID : CVE-2019-12676** | N/A | H-CIS-ASA_-221019/643 |
| Improper Handling of Exceptional Conditions | 02-10-2019 | 4 | A vulnerability in the Secure Sockets Layer (SSL) VPN feature of Cisco Adaptive Security Appliance (ASA) Software could allow an authenticated, remote attacker to cause a denial of service (DoS) condition that prevents | N/A | H-CIS-ASA_-221019/644 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | the creation of new SSL/Transport Layer Security (TLS) connections to an affected device. The vulnerability is due to incorrect handling of Base64-encoded strings. An attacker could exploit this vulnerability by opening many SSL VPN sessions to an affected device. The attacker would need to have valid user credentials on the affected device to exploit this vulnerability. A successful exploit could allow the attacker to overwrite a special system memory location, which will eventually result in memory allocation errors for new SSL/TLS sessions to the device, preventing successful establishment of these sessions. A reload of the device is required to recover from this condition. Established SSL/TLS connections to the device and SSL/TLS connections through the device are not affected. Note: Although this vulnerability is in the SSL VPN feature, successful exploitation of this vulnerability would affect all new SSL/TLS sessions to the device, including management sessions.<br>**CVE ID : CVE-2019-12677** | | |
| Integer Underflow (Wrap or Wraparound | 02-10-2019 | 5 | A vulnerability in the Session Initiation Protocol (SIP) inspection module of Cisco Adaptive Security Appliance | N/A | H-CIS-ASA_-221019/645 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ) | | | (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper parsing of SIP messages. An attacker could exploit this vulnerability by sending a malicious SIP packet through an affected device. A successful exploit could allow the attacker to trigger an integer underflow, causing the software to try to read unmapped memory and resulting in a crash.<br>**CVE ID : CVE-2019-12678** | | |
| Incorrect Type Conversion or Cast | 02-10-2019 | 4 | A vulnerability in the Secure Copy (SCP) feature of Cisco Adaptive Security Appliance (ASA) Software could allow an authenticated, remote attacker to cause a denial of service (DoS) condition. The vulnerability is due to the use of an incorrect data type for a length variable. An attacker could exploit this vulnerability by initiating the transfer of a large file to an affected device via SCP. To exploit this vulnerability, the attacker would need to have valid privilege level 15 credentials on the affected device. A successful exploit could allow the attacker to cause the length variable to roll over, | N/A | H-CIS-ASA_-221019/646 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | which could cause the affected device to crash.<br>**CVE ID : CVE-2019-12693** | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 02-10-2019 | 4.3 | A vulnerability in the Clientless SSL VPN (WebVPN) portal of Cisco Adaptive Security Appliance (ASA) and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or allow the attacker to access sensitive browser-based information.<br>**CVE ID : CVE-2019-12695** | N/A | H-CIS-ASA_-221019/647 |
| Uncontrolled Resource Consumption | 02-10-2019 | 7.8 | A vulnerability in the WebVPN feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause increased CPU utilization on an affected | N/A | H-CIS-ASA_-221019/648 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | device. The vulnerability is due to excessive processing load for a specific WebVPN HTTP page request. An attacker could exploit this vulnerability by sending multiple WebVPN HTTP page load requests for a specific URL. A successful exploit could allow the attacker to increase CPU load on the device, resulting in a denial of service (DoS) condition, which could cause traffic to be delayed through the device.<br>**CVE ID : CVE-2019-12698** | | |
| Uncontrolled Resource Consumption | 02-10-2019 | 7.8 | A vulnerability in the Internet Key Exchange version 1 (IKEv1) feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to improper management of system memory. An attacker could exploit this vulnerability by sending malicious IKEv1 traffic to an affected device. The attacker does not need valid credentials to authenticate the VPN session, nor does the attacker's source address need to match a peer statement in the crypto map applied to the ingress interface of the affected device. An | N/A | H-CIS-ASA_-221019/649 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | exploit could allow the attacker to exhaust system memory resources, leading to a reload of an affected device.<br>**CVE ID : CVE-2019-15256** | | |
| **asa_5520** | | | | | |
| Improper Input Validation | 02-10-2019 | 5 | A vulnerability in the FTP inspection engine of Cisco Adaptive Security (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of FTP data. An attacker could exploit this vulnerability by sending malicious FTP traffic through an affected device. A successful exploit could allow the attacker to cause a DoS condition on the affected device.<br>**CVE ID : CVE-2019-12673** | N/A | H-CIS-ASA_-221019/650 |
| Improper Input Validation | 02-10-2019 | 3.3 | A vulnerability in the Open Shortest Path First (OSPF) implementation of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability exists because the affected | N/A | H-CIS-ASA_-221019/651 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | software improperly parses certain options in OSPF link-state advertisement (LSA) type 11 packets. An attacker could exploit this vulnerability by sending a crafted LSA type 11 OSPF packet to an affected device. A successful exploit could allow the attacker to cause a reload of the affected device, resulting in a DoS condition for client traffic that is traversing the device.<br>**CVE ID : CVE-2019-12676** | | |
| Improper Handling of Exceptional Conditions | 02-10-2019 | 4 | A vulnerability in the Secure Sockets Layer (SSL) VPN feature of Cisco Adaptive Security Appliance (ASA) Software could allow an authenticated, remote attacker to cause a denial of service (DoS) condition that prevents the creation of new SSL/Transport Layer Security (TLS) connections to an affected device. The vulnerability is due to incorrect handling of Base64-encoded strings. An attacker could exploit this vulnerability by opening many SSL VPN sessions to an affected device. The attacker would need to have valid user credentials on the affected device to exploit this vulnerability. A successful exploit could allow the attacker to overwrite a special system memory location, which will eventually result in memory allocation errors for | N/A | H-CIS-ASA_-221019/652 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | new SSL/TLS sessions to the device, preventing successful establishment of these sessions. A reload of the device is required to recover from this condition. Established SSL/TLS connections to the device and SSL/TLS connections through the device are not affected. Note: Although this vulnerability is in the SSL VPN feature, successful exploitation of this vulnerability would affect all new SSL/TLS sessions to the device, including management sessions.<br>**CVE ID : CVE-2019-12677** | | |
| Integer Underflow (Wrap or Wraparound) | 02-10-2019 | 5 | A vulnerability in the Session Initiation Protocol (SIP) inspection module of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper parsing of SIP messages. An attacker could exploit this vulnerability by sending a malicious SIP packet through an affected device. A successful exploit could allow the attacker to trigger an integer underflow, causing the software to try to read unmapped memory and | N/A | H-CIS-ASA_-221019/653 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | resulting in a crash.<br>**CVE ID : CVE-2019-12678** | | |
| Incorrect Type Conversion or Cast | 02-10-2019 | 4 | A vulnerability in the Secure Copy (SCP) feature of Cisco Adaptive Security Appliance (ASA) Software could allow an authenticated, remote attacker to cause a denial of service (DoS) condition. The vulnerability is due to the use of an incorrect data type for a length variable. An attacker could exploit this vulnerability by initiating the transfer of a large file to an affected device via SCP. To exploit this vulnerability, the attacker would need to have valid privilege level 15 credentials on the affected device. A successful exploit could allow the attacker to cause the length variable to roll over, which could cause the affected device to crash.<br>**CVE ID : CVE-2019-12693** | N/A | H-CIS-ASA_-221019/654 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 02-10-2019 | 4.3 | A vulnerability in the Clientless SSL VPN (WebVPN) portal of Cisco Adaptive Security Appliance (ASA) and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. The vulnerability is due to insufficient validation of user- | N/A | H-CIS-ASA_-221019/655 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | supplied input by the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or allow the attacker to access sensitive browser-based information.<br>**CVE ID : CVE-2019-12695** | | |
| Uncontrolled Resource Consumption | 02-10-2019 | 7.8 | A vulnerability in the WebVPN feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause increased CPU utilization on an affected device. The vulnerability is due to excessive processing load for a specific WebVPN HTTP page request. An attacker could exploit this vulnerability by sending multiple WebVPN HTTP page load requests for a specific URL. A successful exploit could allow the attacker to increase CPU load on the device, resulting in a denial of service (DoS) condition, which could cause traffic to be delayed through the device.<br>**CVE ID : CVE-2019-12698** | N/A | H-CIS-ASA_-221019/656 |
| Uncontrolled | 02-10-2019 | 7.8 | A vulnerability in the Internet | N/A | H-CIS-ASA_- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Resource Consumption | | | Key Exchange version 1 (IKEv1) feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to improper management of system memory. An attacker could exploit this vulnerability by sending malicious IKEv1 traffic to an affected device. The attacker does not need valid credentials to authenticate the VPN session, nor does the attacker's source address need to match a peer statement in the crypto map applied to the ingress interface of the affected device. An exploit could allow the attacker to exhaust system memory resources, leading to a reload of an affected device.<br>**CVE ID : CVE-2019-15256** | | 221019/657 |
| **asa_5525-x** | | | | | |
| Improper Input Validation | 02-10-2019 | 5 | A vulnerability in the FTP inspection engine of Cisco Adaptive Security (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The | N/A | H-CIS-ASA_-221019/658 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | vulnerability is due to insufficient validation of FTP data. An attacker could exploit this vulnerability by sending malicious FTP traffic through an affected device. A successful exploit could allow the attacker to cause a DoS condition on the affected device.<br>**CVE ID : CVE-2019-12673** | | |
| Improper Input Validation | 02-10-2019 | 3.3 | A vulnerability in the Open Shortest Path First (OSPF) implementation of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability exists because the affected software improperly parses certain options in OSPF link-state advertisement (LSA) type 11 packets. An attacker could exploit this vulnerability by sending a crafted LSA type 11 OSPF packet to an affected device. A successful exploit could allow the attacker to cause a reload of the affected device, resulting in a DoS condition for client traffic that is traversing the device.<br>**CVE ID : CVE-2019-12676** | N/A | H-CIS-ASA_-221019/659 |
| Improper Handling of | 02-10-2019 | 4 | A vulnerability in the Secure Sockets Layer (SSL) VPN | N/A | H-CIS-ASA_-221019/660 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Exceptional Conditions | | | feature of Cisco Adaptive Security Appliance (ASA) Software could allow an authenticated, remote attacker to cause a denial of service (DoS) condition that prevents the creation of new SSL/Transport Layer Security (TLS) connections to an affected device. The vulnerability is due to incorrect handling of Base64-encoded strings. An attacker could exploit this vulnerability by opening many SSL VPN sessions to an affected device. The attacker would need to have valid user credentials on the affected device to exploit this vulnerability. A successful exploit could allow the attacker to overwrite a special system memory location, which will eventually result in memory allocation errors for new SSL/TLS sessions to the device, preventing successful establishment of these sessions. A reload of the device is required to recover from this condition. Established SSL/TLS connections to the device and SSL/TLS connections through the device are not affected. Note: Although this vulnerability is in the SSL VPN feature, successful exploitation of this vulnerability would affect all new SSL/TLS sessions to the device, including management | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | sessions.<br>**CVE ID : CVE-2019-12677** | | |
| Integer Underflow (Wrap or Wraparound) | 02-10-2019 | 5 | A vulnerability in the Session Initiation Protocol (SIP) inspection module of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper parsing of SIP messages. An attacker could exploit this vulnerability by sending a malicious SIP packet through an affected device. A successful exploit could allow the attacker to trigger an integer underflow, causing the software to try to read unmapped memory and resulting in a crash.<br>**CVE ID : CVE-2019-12678** | N/A | H-CIS-ASA_-221019/661 |
| Incorrect Type Conversion or Cast | 02-10-2019 | 4 | A vulnerability in the Secure Copy (SCP) feature of Cisco Adaptive Security Appliance (ASA) Software could allow an authenticated, remote attacker to cause a denial of service (DoS) condition. The vulnerability is due to the use of an incorrect data type for a length variable. An attacker could exploit this vulnerability by initiating the transfer of a large file to an affected device via SCP. To exploit this | N/A | H-CIS-ASA_-221019/662 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | vulnerability, the attacker would need to have valid privilege level 15 credentials on the affected device. A successful exploit could allow the attacker to cause the length variable to roll over, which could cause the affected device to crash.<br>**CVE ID : CVE-2019-12693** | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 02-10-2019 | 4.3 | A vulnerability in the Clientless SSL VPN (WebVPN) portal of Cisco Adaptive Security Appliance (ASA) and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or allow the attacker to access sensitive browser-based information.<br>**CVE ID : CVE-2019-12695** | N/A | H-CIS-ASA_-221019/663 |
| Uncontrolled Resource | 02-10-2019 | 7.8 | A vulnerability in the WebVPN feature of Cisco Adaptive | N/A | H-CIS-ASA_-221019/664 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Consumption | | | Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause increased CPU utilization on an affected device. The vulnerability is due to excessive processing load for a specific WebVPN HTTP page request. An attacker could exploit this vulnerability by sending multiple WebVPN HTTP page load requests for a specific URL. A successful exploit could allow the attacker to increase CPU load on the device, resulting in a denial of service (DoS) condition, which could cause traffic to be delayed through the device.<br>**CVE ID : CVE-2019-12698** | | |
| Uncontrolled Resource Consumption | 02-10-2019 | 7.8 | A vulnerability in the Internet Key Exchange version 1 (IKEv1) feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to improper management of system memory. An attacker could exploit this vulnerability by sending malicious IKEv1 traffic to an affected device. The attacker does not need | N/A | H-CIS-ASA_-221019/665 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | valid credentials to authenticate the VPN session, nor does the attacker's source address need to match a peer statement in the crypto map applied to the ingress interface of the affected device. An exploit could allow the attacker to exhaust system memory resources, leading to a reload of an affected device.<br>**CVE ID : CVE-2019-15256** | | |
| **asa_5550** | | | | | |
| Improper Input Validation | 02-10-2019 | 5 | A vulnerability in the FTP inspection engine of Cisco Adaptive Security (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of FTP data. An attacker could exploit this vulnerability by sending malicious FTP traffic through an affected device. A successful exploit could allow the attacker to cause a DoS condition on the affected device.<br>**CVE ID : CVE-2019-12673** | N/A | H-CIS-ASA_-221019/666 |
| Improper Input Validation | 02-10-2019 | 3.3 | A vulnerability in the Open Shortest Path First (OSPF) implementation of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense | N/A | H-CIS-ASA_-221019/667 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | (FTD) Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability exists because the affected software improperly parses certain options in OSPF link-state advertisement (LSA) type 11 packets. An attacker could exploit this vulnerability by sending a crafted LSA type 11 OSPF packet to an affected device. A successful exploit could allow the attacker to cause a reload of the affected device, resulting in a DoS condition for client traffic that is traversing the device.<br>**CVE ID : CVE-2019-12676** | | |
| Improper Handling of Exceptional Conditions | 02-10-2019 | 4 | A vulnerability in the Secure Sockets Layer (SSL) VPN feature of Cisco Adaptive Security Appliance (ASA) Software could allow an authenticated, remote attacker to cause a denial of service (DoS) condition that prevents the creation of new SSL/Transport Layer Security (TLS) connections to an affected device. The vulnerability is due to incorrect handling of Base64-encoded strings. An attacker could exploit this vulnerability by opening many SSL VPN sessions to an affected device. The attacker would need to have valid user credentials on | N/A | H-CIS-ASA_-221019/668 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | the affected device to exploit this vulnerability. A successful exploit could allow the attacker to overwrite a special system memory location, which will eventually result in memory allocation errors for new SSL/TLS sessions to the device, preventing successful establishment of these sessions. A reload of the device is required to recover from this condition. Established SSL/TLS connections to the device and SSL/TLS connections through the device are not affected. Note: Although this vulnerability is in the SSL VPN feature, successful exploitation of this vulnerability would affect all new SSL/TLS sessions to the device, including management sessions.<br>**CVE ID : CVE-2019-12677** | | |
| Integer Underflow (Wrap or Wraparound) | 02-10-2019 | 5 | A vulnerability in the Session Initiation Protocol (SIP) inspection module of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper parsing of SIP messages. An attacker could exploit this vulnerability by sending a malicious SIP packet | N/A | H-CIS-ASA_-221019/669 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | through an affected device. A successful exploit could allow the attacker to trigger an integer underflow, causing the software to try to read unmapped memory and resulting in a crash.<br>**CVE ID : CVE-2019-12678** | | |
| Incorrect Type Conversion or Cast | 02-10-2019 | 4 | A vulnerability in the Secure Copy (SCP) feature of Cisco Adaptive Security Appliance (ASA) Software could allow an authenticated, remote attacker to cause a denial of service (DoS) condition. The vulnerability is due to the use of an incorrect data type for a length variable. An attacker could exploit this vulnerability by initiating the transfer of a large file to an affected device via SCP. To exploit this vulnerability, the attacker would need to have valid privilege level 15 credentials on the affected device. A successful exploit could allow the attacker to cause the length variable to roll over, which could cause the affected device to crash.<br>**CVE ID : CVE-2019-12693** | N/A | H-CIS-ASA_-221019/670 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 02-10-2019 | 4.3 | A vulnerability in the Clientless SSL VPN (WebVPN) portal of Cisco Adaptive Security Appliance (ASA) and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct a | N/A | H-CIS-ASA_-221019/671 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or allow the attacker to access sensitive browser-based information.<br>**CVE ID : CVE-2019-12695** | | |
| Uncontrolled Resource Consumption | 02-10-2019 | 7.8 | A vulnerability in the WebVPN feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause increased CPU utilization on an affected device. The vulnerability is due to excessive processing load for a specific WebVPN HTTP page request. An attacker could exploit this vulnerability by sending multiple WebVPN HTTP page load requests for a specific URL. A successful exploit could allow the attacker to increase CPU load on the device, resulting in a denial of service (DoS) | N/A | H-CIS-ASA_-221019/672 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | condition, which could cause traffic to be delayed through the device.<br>**CVE ID : CVE-2019-12698** | | |
| Uncontrolled Resource Consumption | 02-10-2019 | 7.8 | A vulnerability in the Internet Key Exchange version 1 (IKEv1) feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to improper management of system memory. An attacker could exploit this vulnerability by sending malicious IKEv1 traffic to an affected device. The attacker does not need valid credentials to authenticate the VPN session, nor does the attacker's source address need to match a peer statement in the crypto map applied to the ingress interface of the affected device. An exploit could allow the attacker to exhaust system memory resources, leading to a reload of an affected device.<br>**CVE ID : CVE-2019-15256** | N/A | H-CIS-ASA_-221019/673 |
| **asa_5555-x** | | | | | |
| Improper Input Validation | 02-10-2019 | 5 | A vulnerability in the FTP inspection engine of Cisco Adaptive Security (ASA) Software and Cisco Firepower Threat Defense (FTD) | N/A | H-CIS-ASA_-221019/674 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of FTP data. An attacker could exploit this vulnerability by sending malicious FTP traffic through an affected device. A successful exploit could allow the attacker to cause a DoS condition on the affected device.<br>**CVE ID : CVE-2019-12673** | | |
| Improper Input Validation | 02-10-2019 | 3.3 | A vulnerability in the Open Shortest Path First (OSPF) implementation of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability exists because the affected software improperly parses certain options in OSPF link-state advertisement (LSA) type 11 packets. An attacker could exploit this vulnerability by sending a crafted LSA type 11 OSPF packet to an affected device. A successful exploit could allow the attacker to cause a reload of the affected device, resulting in a DoS condition for client traffic that | N/A | H-CIS-ASA_-221019/675 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | is traversing the device.<br>**CVE ID : CVE-2019-12676** | | |
| Improper Handling of Exceptional Conditions | 02-10-2019 | 4 | A vulnerability in the Secure Sockets Layer (SSL) VPN feature of Cisco Adaptive Security Appliance (ASA) Software could allow an authenticated, remote attacker to cause a denial of service (DoS) condition that prevents the creation of new SSL/Transport Layer Security (TLS) connections to an affected device. The vulnerability is due to incorrect handling of Base64-encoded strings. An attacker could exploit this vulnerability by opening many SSL VPN sessions to an affected device. The attacker would need to have valid user credentials on the affected device to exploit this vulnerability. A successful exploit could allow the attacker to overwrite a special system memory location, which will eventually result in memory allocation errors for new SSL/TLS sessions to the device, preventing successful establishment of these sessions. A reload of the device is required to recover from this condition. Established SSL/TLS connections to the device and SSL/TLS connections through the device are not affected. Note: Although this vulnerability is in the SSL VPN feature, | N/A | H-CIS-ASA_-221019/676 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | successful exploitation of this vulnerability would affect all new SSL/TLS sessions to the device, including management sessions.<br>**CVE ID : CVE-2019-12677** | | |
| Integer Underflow (Wrap or Wraparound) | 02-10-2019 | 5 | A vulnerability in the Session Initiation Protocol (SIP) inspection module of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper parsing of SIP messages. An attacker could exploit this vulnerability by sending a malicious SIP packet through an affected device. A successful exploit could allow the attacker to trigger an integer underflow, causing the software to try to read unmapped memory and resulting in a crash.<br>**CVE ID : CVE-2019-12678** | N/A | H-CIS-ASA_-221019/677 |
| Incorrect Type Conversion or Cast | 02-10-2019 | 4 | A vulnerability in the Secure Copy (SCP) feature of Cisco Adaptive Security Appliance (ASA) Software could allow an authenticated, remote attacker to cause a denial of service (DoS) condition. The vulnerability is due to the use of an incorrect data type for a length variable. An attacker | N/A | H-CIS-ASA_-221019/678 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | could exploit this vulnerability by initiating the transfer of a large file to an affected device via SCP. To exploit this vulnerability, the attacker would need to have valid privilege level 15 credentials on the affected device. A successful exploit could allow the attacker to cause the length variable to roll over, which could cause the affected device to crash.<br>**CVE ID : CVE-2019-12693** | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 02-10-2019 | 4.3 | A vulnerability in the Clientless SSL VPN (WebVPN) portal of Cisco Adaptive Security Appliance (ASA) and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or allow the attacker to access sensitive | N/A | H-CIS-ASA_-221019/679 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | browser-based information.<br>**CVE ID : CVE-2019-12695** | | |
| Uncontrolled Resource Consumption | 02-10-2019 | 7.8 | A vulnerability in the WebVPN feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause increased CPU utilization on an affected device. The vulnerability is due to excessive processing load for a specific WebVPN HTTP page request. An attacker could exploit this vulnerability by sending multiple WebVPN HTTP page load requests for a specific URL. A successful exploit could allow the attacker to increase CPU load on the device, resulting in a denial of service (DoS) condition, which could cause traffic to be delayed through the device.<br>**CVE ID : CVE-2019-12698** | N/A | H-CIS-ASA_-221019/680 |
| Uncontrolled Resource Consumption | 02-10-2019 | 7.8 | A vulnerability in the Internet Key Exchange version 1 (IKEv1) feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to improper management | N/A | H-CIS-ASA_-221019/681 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | of system memory. An attacker could exploit this vulnerability by sending malicious IKEv1 traffic to an affected device. The attacker does not need valid credentials to authenticate the VPN session, nor does the attacker's source address need to match a peer statement in the crypto map applied to the ingress interface of the affected device. An exploit could allow the attacker to exhaust system memory resources, leading to a reload of an affected device.<br>**CVE ID : CVE-2019-15256** | | |
| **asa_5580** | | | | | |
| Improper Input Validation | 02-10-2019 | 5 | A vulnerability in the FTP inspection engine of Cisco Adaptive Security (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of FTP data. An attacker could exploit this vulnerability by sending malicious FTP traffic through an affected device. A successful exploit could allow the attacker to cause a DoS condition on the affected device.<br>**CVE ID : CVE-2019-12673** | N/A | H-CIS-ASA_-221019/682 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Input Validation | 02-10-2019 | 3.3 | A vulnerability in the Open Shortest Path First (OSPF) implementation of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability exists because the affected software improperly parses certain options in OSPF link-state advertisement (LSA) type 11 packets. An attacker could exploit this vulnerability by sending a crafted LSA type 11 OSPF packet to an affected device. A successful exploit could allow the attacker to cause a reload of the affected device, resulting in a DoS condition for client traffic that is traversing the device.<br>**CVE ID : CVE-2019-12676** | N/A | H-CIS-ASA_-221019/683 |
| Improper Handling of Exceptional Conditions | 02-10-2019 | 4 | A vulnerability in the Secure Sockets Layer (SSL) VPN feature of Cisco Adaptive Security Appliance (ASA) Software could allow an authenticated, remote attacker to cause a denial of service (DoS) condition that prevents the creation of new SSL/Transport Layer Security (TLS) connections to an affected device. The vulnerability is due to incorrect handling of Base64- | N/A | H-CIS-ASA_-221019/684 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | encoded strings. An attacker could exploit this vulnerability by opening many SSL VPN sessions to an affected device. The attacker would need to have valid user credentials on the affected device to exploit this vulnerability. A successful exploit could allow the attacker to overwrite a special system memory location, which will eventually result in memory allocation errors for new SSL/TLS sessions to the device, preventing successful establishment of these sessions. A reload of the device is required to recover from this condition. Established SSL/TLS connections to the device and SSL/TLS connections through the device are not affected. Note: Although this vulnerability is in the SSL VPN feature, successful exploitation of this vulnerability would affect all new SSL/TLS sessions to the device, including management sessions.<br>**CVE ID : CVE-2019-12677** | | |
| Integer Underflow (Wrap or Wraparound) | 02-10-2019 | 5 | A vulnerability in the Session Initiation Protocol (SIP) inspection module of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an | N/A | H-CIS-ASA_-221019/685 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | affected device. The vulnerability is due to improper parsing of SIP messages. An attacker could exploit this vulnerability by sending a malicious SIP packet through an affected device. A successful exploit could allow the attacker to trigger an integer underflow, causing the software to try to read unmapped memory and resulting in a crash.<br>**CVE ID : CVE-2019-12678** | | |
| Incorrect Type Conversion or Cast | 02-10-2019 | 4 | A vulnerability in the Secure Copy (SCP) feature of Cisco Adaptive Security Appliance (ASA) Software could allow an authenticated, remote attacker to cause a denial of service (DoS) condition. The vulnerability is due to the use of an incorrect data type for a length variable. An attacker could exploit this vulnerability by initiating the transfer of a large file to an affected device via SCP. To exploit this vulnerability, the attacker would need to have valid privilege level 15 credentials on the affected device. A successful exploit could allow the attacker to cause the length variable to roll over, which could cause the affected device to crash.<br>**CVE ID : CVE-2019-12693** | N/A | H-CIS-ASA_-221019/686 |
| Improper Neutralizatio | 02-10-2019 | 4.3 | A vulnerability in the Clientless SSL VPN (WebVPN) | N/A | H-CIS-ASA_-221019/687 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| n of Input During Web Page Generation ('Cross-site Scripting') | | | portal of Cisco Adaptive Security Appliance (ASA) and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or allow the attacker to access sensitive browser-based information.<br>**CVE ID : CVE-2019-12695** | | |
| Uncontrolled Resource Consumption | 02-10-2019 | 7.8 | A vulnerability in the WebVPN feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause increased CPU utilization on an affected device. The vulnerability is due to excessive processing load for a specific WebVPN HTTP page request. An attacker could exploit this vulnerability by sending multiple WebVPN | N/A | H-CIS-ASA_-221019/688 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | HTTP page load requests for a specific URL. A successful exploit could allow the attacker to increase CPU load on the device, resulting in a denial of service (DoS) condition, which could cause traffic to be delayed through the device.<br>**CVE ID : CVE-2019-12698** | | |
| Uncontrolled Resource Consumption | 02-10-2019 | 7.8 | A vulnerability in the Internet Key Exchange version 1 (IKEv1) feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to improper management of system memory. An attacker could exploit this vulnerability by sending malicious IKEv1 traffic to an affected device. The attacker does not need valid credentials to authenticate the VPN session, nor does the attacker's source address need to match a peer statement in the crypto map applied to the ingress interface of the affected device. An exploit could allow the attacker to exhaust system memory resources, leading to a reload of an affected device.<br>**CVE ID : CVE-2019-15256** | N/A | H-CIS-ASA_-221019/689 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **asa_5585-x** | | | | | |
| Improper Input Validation | 02-10-2019 | 5 | A vulnerability in the FTP inspection engine of Cisco Adaptive Security (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of FTP data. An attacker could exploit this vulnerability by sending malicious FTP traffic through an affected device. A successful exploit could allow the attacker to cause a DoS condition on the affected device.<br>**CVE ID : CVE-2019-12673** | N/A | H-CIS-ASA_-221019/690 |
| Improper Input Validation | 02-10-2019 | 3.3 | A vulnerability in the Open Shortest Path First (OSPF) implementation of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability exists because the affected software improperly parses certain options in OSPF link-state advertisement (LSA) type 11 packets. An attacker could exploit this vulnerability by | N/A | H-CIS-ASA_-221019/691 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | sending a crafted LSA type 11 OSPF packet to an affected device. A successful exploit could allow the attacker to cause a reload of the affected device, resulting in a DoS condition for client traffic that is traversing the device.<br>**CVE ID : CVE-2019-12676** | | |
| Improper Handling of Exceptional Conditions | 02-10-2019 | 4 | A vulnerability in the Secure Sockets Layer (SSL) VPN feature of Cisco Adaptive Security Appliance (ASA) Software could allow an authenticated, remote attacker to cause a denial of service (DoS) condition that prevents the creation of new SSL/Transport Layer Security (TLS) connections to an affected device. The vulnerability is due to incorrect handling of Base64-encoded strings. An attacker could exploit this vulnerability by opening many SSL VPN sessions to an affected device. The attacker would need to have valid user credentials on the affected device to exploit this vulnerability. A successful exploit could allow the attacker to overwrite a special system memory location, which will eventually result in memory allocation errors for new SSL/TLS sessions to the device, preventing successful establishment of these sessions. A reload of the device is required to recover from | N/A | H-CIS-ASA_-221019/692 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | this condition. Established SSL/TLS connections to the device and SSL/TLS connections through the device are not affected. Note: Although this vulnerability is in the SSL VPN feature, successful exploitation of this vulnerability would affect all new SSL/TLS sessions to the device, including management sessions.<br>**CVE ID : CVE-2019-12677** | | |
| Integer Underflow (Wrap or Wraparound) | 02-10-2019 | 5 | A vulnerability in the Session Initiation Protocol (SIP) inspection module of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper parsing of SIP messages. An attacker could exploit this vulnerability by sending a malicious SIP packet through an affected device. A successful exploit could allow the attacker to trigger an integer underflow, causing the software to try to read unmapped memory and resulting in a crash.<br>**CVE ID : CVE-2019-12678** | N/A | H-CIS-ASA_-221019/693 |
| Incorrect Type Conversion | 02-10-2019 | 4 | A vulnerability in the Secure Copy (SCP) feature of Cisco Adaptive Security Appliance | N/A | H-CIS-ASA_-221019/694 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| or Cast | | | (ASA) Software could allow an authenticated, remote attacker to cause a denial of service (DoS) condition. The vulnerability is due to the use of an incorrect data type for a length variable. An attacker could exploit this vulnerability by initiating the transfer of a large file to an affected device via SCP. To exploit this vulnerability, the attacker would need to have valid privilege level 15 credentials on the affected device. A successful exploit could allow the attacker to cause the length variable to roll over, which could cause the affected device to crash.<br>**CVE ID : CVE-2019-12693** | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 02-10-2019 | 4.3 | A vulnerability in the Clientless SSL VPN (WebVPN) portal of Cisco Adaptive Security Appliance (ASA) and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a | N/A | H-CIS-ASA_-221019/695 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or allow the attacker to access sensitive browser-based information.<br>**CVE ID : CVE-2019-12695** | | |
| Uncontrolled Resource Consumption | 02-10-2019 | 7.8 | A vulnerability in the WebVPN feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause increased CPU utilization on an affected device. The vulnerability is due to excessive processing load for a specific WebVPN HTTP page request. An attacker could exploit this vulnerability by sending multiple WebVPN HTTP page load requests for a specific URL. A successful exploit could allow the attacker to increase CPU load on the device, resulting in a denial of service (DoS) condition, which could cause traffic to be delayed through the device.<br>**CVE ID : CVE-2019-12698** | N/A | H-CIS-ASA_-221019/696 |
| **firepower_9300** | | | | | |
| Improper Encoding or Escaping of Output | 02-10-2019 | 7.2 | Multiple vulnerabilities in the multi-instance feature of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to escape the container for their | N/A | H-CIS-FIRE-221019/697 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | FTD instance and execute commands with root privileges in the host namespace. These vulnerabilities are due to insufficient protections on the underlying filesystem. An attacker could exploit these vulnerabilities by modifying critical files on the underlying filesystem. A successful exploit could allow the attacker to execute commands with root privileges within the host namespace. This could allow the attacker to impact other running FTD instances.<br>**CVE ID : CVE-2019-12674** | | |
| Improper Encoding or Escaping of Output | 02-10-2019 | 7.2 | Multiple vulnerabilities in the multi-instance feature of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to escape the container for their FTD instance and execute commands with root privileges in the host namespace. These vulnerabilities are due to insufficient protections on the underlying filesystem. An attacker could exploit these vulnerabilities by modifying critical files on the underlying filesystem. A successful exploit could allow the attacker to execute commands with root privileges within the host namespace. This could allow the attacker to impact other | N/A | H-CIS-FIRE-221019/698 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | running FTD instances.<br>**CVE ID : CVE-2019-12675** | | |
| Improper Input Validation | 02-10-2019 | 5 | Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details section of this advisory.<br>**CVE ID : CVE-2019-12696** | N/A | H-CIS-FIRE-221019/699 |
| Improper Input Validation | 02-10-2019 | 5 | Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details section of this advisory.<br>**CVE ID : CVE-2019-12697** | N/A | H-CIS-FIRE-221019/700 |
| Improper Input Validation | 02-10-2019 | 7.2 | Multiple vulnerabilities in the CLI of Cisco FXOS Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute commands on the underlying operating system (OS) with root privileges. These vulnerabilities are due to insufficient input validation. An attacker could exploit these vulnerabilities by including | N/A | H-CIS-FIRE-221019/701 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | crafted arguments to specific CLI commands. A successful exploit could allow the attacker to execute commands on the underlying OS with root privileges.<br>**CVE ID : CVE-2019-12699** | | |
| Uncontrolled Resource Consumption | 02-10-2019 | 6.8 | A vulnerability in the configuration of the Pluggable Authentication Module (PAM) used in Cisco Firepower Threat Defense (FTD) Software, Cisco Firepower Management Center (FMC) Software, and Cisco FXOS Software could allow an authenticated, remote attacker to cause a denial of service (DoS) condition. The vulnerability is due to improper resource management in the context of user session management. An attacker could exploit this vulnerability by connecting to an affected system and performing many simultaneous successful Secure Shell (SSH) logins. A successful exploit could allow the attacker to exhaust system resources and cause the device to reload, resulting in a DoS condition. To exploit this vulnerability, the attacker needs valid user credentials on the system.<br>**CVE ID : CVE-2019-12700** | N/A | H-CIS-FIRE-221019/702 |
| **firepower_4115** | | | | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Encoding or Escaping of Output | 02-10-2019 | 7.2 | Multiple vulnerabilities in the multi-instance feature of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to escape the container for their FTD instance and execute commands with root privileges in the host namespace. These vulnerabilities are due to insufficient protections on the underlying filesystem. An attacker could exploit these vulnerabilities by modifying critical files on the underlying filesystem. A successful exploit could allow the attacker to execute commands with root privileges within the host namespace. This could allow the attacker to impact other running FTD instances.<br>**CVE ID : CVE-2019-12674** | N/A | H-CIS-FIRE-221019/703 |
| Improper Encoding or Escaping of Output | 02-10-2019 | 7.2 | Multiple vulnerabilities in the multi-instance feature of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to escape the container for their FTD instance and execute commands with root privileges in the host namespace. These vulnerabilities are due to insufficient protections on the underlying filesystem. An attacker could exploit these vulnerabilities by modifying critical files on the underlying filesystem. A successful exploit | N/A | H-CIS-FIRE-221019/704 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | could allow the attacker to execute commands with root privileges within the host namespace. This could allow the attacker to impact other running FTD instances.<br>**CVE ID : CVE-2019-12675** | | |
| Improper Input Validation | 02-10-2019 | 5 | Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details section of this advisory.<br>**CVE ID : CVE-2019-12696** | N/A | H-CIS-FIRE-221019/705 |
| Improper Input Validation | 02-10-2019 | 5 | Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details section of this advisory.<br>**CVE ID : CVE-2019-12697** | N/A | H-CIS-FIRE-221019/706 |
| **firepower_4125** | | | | | |
| Improper Encoding or Escaping of Output | 02-10-2019 | 7.2 | Multiple vulnerabilities in the multi-instance feature of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to escape the container for their FTD instance and execute | N/A | H-CIS-FIRE-221019/707 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | commands with root privileges in the host namespace. These vulnerabilities are due to insufficient protections on the underlying filesystem. An attacker could exploit these vulnerabilities by modifying critical files on the underlying filesystem. A successful exploit could allow the attacker to execute commands with root privileges within the host namespace. This could allow the attacker to impact other running FTD instances.<br>**CVE ID : CVE-2019-12674** | | |
| Improper Encoding or Escaping of Output | 02-10-2019 | 7.2 | Multiple vulnerabilities in the multi-instance feature of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to escape the container for their FTD instance and execute commands with root privileges in the host namespace. These vulnerabilities are due to insufficient protections on the underlying filesystem. An attacker could exploit these vulnerabilities by modifying critical files on the underlying filesystem. A successful exploit could allow the attacker to execute commands with root privileges within the host namespace. This could allow the attacker to impact other running FTD instances. | N/A | H-CIS-FIRE-221019/708 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2019-12675** | | |
| Improper Input Validation | 02-10-2019 | 5 | Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details section of this advisory.<br>**CVE ID : CVE-2019-12696** | N/A | H-CIS-FIRE-221019/709 |
| Improper Input Validation | 02-10-2019 | 5 | Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details section of this advisory.<br>**CVE ID : CVE-2019-12697** | N/A | H-CIS-FIRE-221019/710 |
| **firepower_4145** | | | | | |
| Improper Encoding or Escaping of Output | 02-10-2019 | 7.2 | Multiple vulnerabilities in the multi-instance feature of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to escape the container for their FTD instance and execute commands with root privileges in the host namespace. These vulnerabilities are due to insufficient protections on the underlying filesystem. An | N/A | H-CIS-FIRE-221019/711 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | attacker could exploit these vulnerabilities by modifying critical files on the underlying filesystem. A successful exploit could allow the attacker to execute commands with root privileges within the host namespace. This could allow the attacker to impact other running FTD instances.<br>**CVE ID : CVE-2019-12674** | | |
| Improper Encoding or Escaping of Output | 02-10-2019 | 7.2 | Multiple vulnerabilities in the multi-instance feature of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to escape the container for their FTD instance and execute commands with root privileges in the host namespace. These vulnerabilities are due to insufficient protections on the underlying filesystem. An attacker could exploit these vulnerabilities by modifying critical files on the underlying filesystem. A successful exploit could allow the attacker to execute commands with root privileges within the host namespace. This could allow the attacker to impact other running FTD instances.<br>**CVE ID : CVE-2019-12675** | N/A | H-CIS-FIRE-221019/712 |
| Improper Input Validation | 02-10-2019 | 5 | Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote | N/A | H-CIS-FIRE-221019/713 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details section of this advisory.<br>**CVE ID : CVE-2019-12696** | | |
| Improper Input Validation | 02-10-2019 | 5 | Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details section of this advisory.<br>**CVE ID : CVE-2019-12697** | N/A | H-CIS-FIRE-221019/714 |
| **firepower_4110** | | | | | |
| Improper Encoding or Escaping of Output | 02-10-2019 | 7.2 | Multiple vulnerabilities in the multi-instance feature of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to escape the container for their FTD instance and execute commands with root privileges in the host namespace. These vulnerabilities are due to insufficient protections on the underlying filesystem. An attacker could exploit these vulnerabilities by modifying critical files on the underlying filesystem. A successful exploit could allow the attacker to execute commands with root privileges within the host | N/A | H-CIS-FIRE-221019/715 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | namespace. This could allow the attacker to impact other running FTD instances.<br>**CVE ID : CVE-2019-12674** | | |
| Improper Encoding or Escaping of Output | 02-10-2019 | 7.2 | Multiple vulnerabilities in the multi-instance feature of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to escape the container for their FTD instance and execute commands with root privileges in the host namespace. These vulnerabilities are due to insufficient protections on the underlying filesystem. An attacker could exploit these vulnerabilities by modifying critical files on the underlying filesystem. A successful exploit could allow the attacker to execute commands with root privileges within the host namespace. This could allow the attacker to impact other running FTD instances.<br>**CVE ID : CVE-2019-12675** | N/A | H-CIS-FIRE-221019/716 |
| Improper Input Validation | 02-10-2019 | 5 | Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details section of this advisory. | N/A | H-CIS-FIRE-221019/717 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2019-12696** | | |
| Improper Input Validation | 02-10-2019 | 5 | Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details section of this advisory.<br>**CVE ID : CVE-2019-12697** | N/A | H-CIS-FIRE-221019/718 |
| **firepower_4120** | | | | | |
| Improper Encoding or Escaping of Output | 02-10-2019 | 7.2 | Multiple vulnerabilities in the multi-instance feature of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to escape the container for their FTD instance and execute commands with root privileges in the host namespace. These vulnerabilities are due to insufficient protections on the underlying filesystem. An attacker could exploit these vulnerabilities by modifying critical files on the underlying filesystem. A successful exploit could allow the attacker to execute commands with root privileges within the host namespace. This could allow the attacker to impact other running FTD instances.<br>**CVE ID : CVE-2019-12674** | N/A | H-CIS-FIRE-221019/719 |
| Improper | 02-10-2019 | 7.2 | Multiple vulnerabilities in the | N/A | H-CIS-FIRE- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Encoding or Escaping of Output | | | multi-instance feature of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to escape the container for their FTD instance and execute commands with root privileges in the host namespace. These vulnerabilities are due to insufficient protections on the underlying filesystem. An attacker could exploit these vulnerabilities by modifying critical files on the underlying filesystem. A successful exploit could allow the attacker to execute commands with root privileges within the host namespace. This could allow the attacker to impact other running FTD instances.<br>**CVE ID : CVE-2019-12675** | | 221019/720 |
| Improper Input Validation | 02-10-2019 | 5 | Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details section of this advisory.<br>**CVE ID : CVE-2019-12696** | N/A | H-CIS-FIRE-221019/721 |
| Improper Input Validation | 02-10-2019 | 5 | Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote | N/A | H-CIS-FIRE-221019/722 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details section of this advisory.<br>**CVE ID : CVE-2019-12697** | | |
| **firepower_4140** | | | | | |
| Improper Encoding or Escaping of Output | 02-10-2019 | 7.2 | Multiple vulnerabilities in the multi-instance feature of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to escape the container for their FTD instance and execute commands with root privileges in the host namespace. These vulnerabilities are due to insufficient protections on the underlying filesystem. An attacker could exploit these vulnerabilities by modifying critical files on the underlying filesystem. A successful exploit could allow the attacker to execute commands with root privileges within the host namespace. This could allow the attacker to impact other running FTD instances.<br>**CVE ID : CVE-2019-12674** | N/A | H-CIS-FIRE-221019/723 |
| Improper Encoding or Escaping of Output | 02-10-2019 | 7.2 | Multiple vulnerabilities in the multi-instance feature of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to escape the container for their FTD instance and execute commands with root | N/A | H-CIS-FIRE-221019/724 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | privileges in the host namespace. These vulnerabilities are due to insufficient protections on the underlying filesystem. An attacker could exploit these vulnerabilities by modifying critical files on the underlying filesystem. A successful exploit could allow the attacker to execute commands with root privileges within the host namespace. This could allow the attacker to impact other running FTD instances.<br>**CVE ID : CVE-2019-12675** | | |
| Improper Input Validation | 02-10-2019 | 5 | Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details section of this advisory.<br>**CVE ID : CVE-2019-12696** | N/A | H-CIS-FIRE-221019/725 |
| Improper Input Validation | 02-10-2019 | 5 | Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details section of this advisory. | N/A | H-CIS-FIRE-221019/726 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2019-12697** | | |
| **firepower_4150** | | | | | |
| Improper Encoding or Escaping of Output | 02-10-2019 | 7.2 | Multiple vulnerabilities in the multi-instance feature of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to escape the container for their FTD instance and execute commands with root privileges in the host namespace. These vulnerabilities are due to insufficient protections on the underlying filesystem. An attacker could exploit these vulnerabilities by modifying critical files on the underlying filesystem. A successful exploit could allow the attacker to execute commands with root privileges within the host namespace. This could allow the attacker to impact other running FTD instances.<br>**CVE ID : CVE-2019-12674** | N/A | H-CIS-FIRE-221019/727 |
| Improper Encoding or Escaping of Output | 02-10-2019 | 7.2 | Multiple vulnerabilities in the multi-instance feature of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to escape the container for their FTD instance and execute commands with root privileges in the host namespace. These vulnerabilities are due to insufficient protections on the underlying filesystem. An attacker could exploit these | N/A | H-CIS-FIRE-221019/728 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | vulnerabilities by modifying critical files on the underlying filesystem. A successful exploit could allow the attacker to execute commands with root privileges within the host namespace. This could allow the attacker to impact other running FTD instances.<br>**CVE ID : CVE-2019-12675** | | |
| Improper Input Validation | 02-10-2019 | 5 | Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details section of this advisory.<br>**CVE ID : CVE-2019-12696** | N/A | H-CIS-FIRE-221019/729 |
| Improper Input Validation | 02-10-2019 | 5 | Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details section of this advisory.<br>**CVE ID : CVE-2019-12697** | N/A | H-CIS-FIRE-221019/730 |
| **asa_5500-x** | | | | | |
| Improper Input Validation | 02-10-2019 | 5 | Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an | N/A | H-CIS-ASA_-221019/731 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | unauthenticated, remote attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details section of this advisory.<br>**CVE ID : CVE-2019-12696** | | |
| Improper Input Validation | 02-10-2019 | 5 | Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details section of this advisory.<br>**CVE ID : CVE-2019-12697** | N/A | H-CIS-ASA_-221019/732 |
| **firepower_1010** | | | | | |
| Improper Input Validation | 02-10-2019 | 5 | Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details section of this advisory.<br>**CVE ID : CVE-2019-12696** | N/A | H-CIS-FIRE-221019/733 |
| Improper Input Validation | 02-10-2019 | 5 | Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured | N/A | H-CIS-FIRE-221019/734 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details section of this advisory.<br>**CVE ID : CVE-2019-12697** | | |
| **firepower_1120** | | | | | |
| Improper Input Validation | 02-10-2019 | 5 | Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details section of this advisory.<br>**CVE ID : CVE-2019-12696** | N/A | H-CIS-FIRE-221019/735 |
| Improper Input Validation | 02-10-2019 | 5 | Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details section of this advisory.<br>**CVE ID : CVE-2019-12697** | N/A | H-CIS-FIRE-221019/736 |
| **firepower_1140** | | | | | |
| Improper Input Validation | 02-10-2019 | 5 | Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for | N/A | H-CIS-FIRE-221019/737 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | RTF and RAR file types. For more information about these vulnerabilities, see the Details section of this advisory.<br>**CVE ID : CVE-2019-12696** | | |
| Improper Input Validation | 02-10-2019 | 5 | Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details section of this advisory.<br>**CVE ID : CVE-2019-12697** | N/A | H-CIS-FIRE-221019/738 |
| **firepower_2110** | | | | | |
| Improper Input Validation | 02-10-2019 | 5 | Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details section of this advisory.<br>**CVE ID : CVE-2019-12696** | N/A | H-CIS-FIRE-221019/739 |
| Improper Input Validation | 02-10-2019 | 5 | Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these | N/A | H-CIS-FIRE-221019/740 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | vulnerabilities, see the Details section of this advisory.<br>**CVE ID : CVE-2019-12697** | | |
| **firepower_2120** | | | | | |
| Improper Input Validation | 02-10-2019 | 5 | Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details section of this advisory.<br>**CVE ID : CVE-2019-12696** | N/A | H-CIS-FIRE-221019/741 |
| Improper Input Validation | 02-10-2019 | 5 | Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details section of this advisory.<br>**CVE ID : CVE-2019-12697** | N/A | H-CIS-FIRE-221019/742 |
| **firepower_2130** | | | | | |
| Improper Input Validation | 02-10-2019 | 5 | Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details | N/A | H-CIS-FIRE-221019/743 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | section of this advisory.<br>**CVE ID : CVE-2019-12696** | | |
| Improper Input Validation | 02-10-2019 | 5 | Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details section of this advisory.<br>**CVE ID : CVE-2019-12697** | N/A | H-CIS-FIRE-221019/744 |
| **firepower_2140** | | | | | |
| Improper Input Validation | 02-10-2019 | 5 | Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details section of this advisory.<br>**CVE ID : CVE-2019-12696** | N/A | H-CIS-FIRE-221019/745 |
| Improper Input Validation | 02-10-2019 | 5 | Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details section of this advisory. | N/A | H-CIS-FIRE-221019/746 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2019-12697** | | |
| **firepower_7000** | | | | | |
| Improper Input Validation | 02-10-2019 | 5 | Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details section of this advisory.<br>**CVE ID : CVE-2019-12696** | N/A | H-CIS-FIRE-221019/747 |
| Improper Input Validation | 02-10-2019 | 5 | Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details section of this advisory.<br>**CVE ID : CVE-2019-12697** | N/A | H-CIS-FIRE-221019/748 |
| **firepower_8000** | | | | | |
| Improper Input Validation | 02-10-2019 | 5 | Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details section of this advisory. | N/A | H-CIS-FIRE-221019/749 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2019-12696** | | |
| Improper Input Validation | 02-10-2019 | 5 | Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details section of this advisory.<br>**CVE ID : CVE-2019-12697** | N/A | H-CIS-FIRE-221019/750 |
| **firepower_threat_defense_for_isr** | | | | | |
| Improper Input Validation | 02-10-2019 | 5 | Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details section of this advisory.<br>**CVE ID : CVE-2019-12696** | N/A | H-CIS-FIRE-221019/751 |
| Improper Input Validation | 02-10-2019 | 5 | Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details section of this advisory.<br>**CVE ID : CVE-2019-12697** | N/A | H-CIS-FIRE-221019/752 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **ftd_virtual** | | | | | |
| Improper Input Validation | 02-10-2019 | 5 | Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details section of this advisory.<br>**CVE ID : CVE-2019-12696** | N/A | H-CIS-FTD_-221019/753 |
| Improper Input Validation | 02-10-2019 | 5 | Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details section of this advisory.<br>**CVE ID : CVE-2019-12697** | N/A | H-CIS-FTD_-221019/754 |
| **isa_3000** | | | | | |
| Improper Input Validation | 02-10-2019 | 5 | Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details section of this advisory.<br>**CVE ID : CVE-2019-12696** | N/A | H-CIS-ISA_-221019/755 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Input Validation | 02-10-2019 | 5 | Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details section of this advisory.<br>**CVE ID : CVE-2019-12697** | N/A | H-CIS-ISA_-221019/756 |
| **ngipsv_for_vmware** | | | | | |
| Improper Input Validation | 02-10-2019 | 5 | Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details section of this advisory.<br>**CVE ID : CVE-2019-12696** | N/A | H-CIS-NGIP-221019/757 |
| Improper Input Validation | 02-10-2019 | 5 | Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details section of this advisory.<br>**CVE ID : CVE-2019-12697** | N/A | H-CIS-NGIP-221019/758 |
| **firepower_1000** | | | | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Input Validation | 02-10-2019 | 7.2 | Multiple vulnerabilities in the CLI of Cisco FXOS Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute commands on the underlying operating system (OS) with root privileges. These vulnerabilities are due to insufficient input validation. An attacker could exploit these vulnerabilities by including crafted arguments to specific CLI commands. A successful exploit could allow the attacker to execute commands on the underlying OS with root privileges.<br>**CVE ID : CVE-2019-12699** | N/A | H-CIS-FIRE-221019/759 |
| Uncontrolled Resource Consumption | 02-10-2019 | 6.8 | A vulnerability in the configuration of the Pluggable Authentication Module (PAM) used in Cisco Firepower Threat Defense (FTD) Software, Cisco Firepower Management Center (FMC) Software, and Cisco FXOS Software could allow an authenticated, remote attacker to cause a denial of service (DoS) condition. The vulnerability is due to improper resource management in the context of user session management. An attacker could exploit this vulnerability by connecting to an affected system and performing many simultaneous successful | N/A | H-CIS-FIRE-221019/760 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Secure Shell (SSH) logins. A successful exploit could allow the attacker to exhaust system resources and cause the device to reload, resulting in a DoS condition. To exploit this vulnerability, the attacker needs valid user credentials on the system.<br>**CVE ID : CVE-2019-12700** | | |
| **firepower_2100** | | | | | |
| Improper Input Validation | 02-10-2019 | 7.2 | Multiple vulnerabilities in the CLI of Cisco FXOS Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute commands on the underlying operating system (OS) with root privileges. These vulnerabilities are due to insufficient input validation. An attacker could exploit these vulnerabilities by including crafted arguments to specific CLI commands. A successful exploit could allow the attacker to execute commands on the underlying OS with root privileges.<br>**CVE ID : CVE-2019-12699** | N/A | H-CIS-FIRE-221019/761 |
| Uncontrolled Resource Consumption | 02-10-2019 | 6.8 | A vulnerability in the configuration of the Pluggable Authentication Module (PAM) used in Cisco Firepower Threat Defense (FTD) Software, Cisco Firepower Management Center (FMC) Software, and Cisco FXOS Software could allow an | N/A | H-CIS-FIRE-221019/762 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | authenticated, remote attacker to cause a denial of service (DoS) condition. The vulnerability is due to improper resource management in the context of user session management. An attacker could exploit this vulnerability by connecting to an affected system and performing many simultaneous successful Secure Shell (SSH) logins. A successful exploit could allow the attacker to exhaust system resources and cause the device to reload, resulting in a DoS condition. To exploit this vulnerability, the attacker needs valid user credentials on the system.<br>**CVE ID : CVE-2019-12700** | | |
| **firepower_4100** | | | | | |
| Improper Input Validation | 02-10-2019 | 7.2 | Multiple vulnerabilities in the CLI of Cisco FXOS Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute commands on the underlying operating system (OS) with root privileges. These vulnerabilities are due to insufficient input validation. An attacker could exploit these vulnerabilities by including crafted arguments to specific CLI commands. A successful exploit could allow the attacker to execute commands | N/A | H-CIS-FIRE-221019/763 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | on the underlying OS with root privileges.<br>**CVE ID : CVE-2019-12699** | | |
| **ic3000_industrial_compute_gateway** | | | | | |
| Uncontrolled Resource Consumption | 02-10-2019 | 4 | A vulnerability in the web-based management interface of Cisco IC3000 Industrial Compute Gateway could allow an authenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability exists because the affected software improperly manages system resources. An attacker could exploit this vulnerability by opening a large number of simultaneous sessions on the web-based management interface of an affected device. A successful exploit could allow the attacker to cause a DoS condition of the web-based management interface, preventing normal management operations.<br>**CVE ID : CVE-2019-12714** | N/A | H-CIS-IC30-221019/764 |
| **asa_5540** | | | | | |
| Uncontrolled Resource Consumption | 02-10-2019 | 7.8 | A vulnerability in the Internet Key Exchange version 1 (IKEv1) feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a reload of an affected device, resulting in | N/A | H-CIS-ASA_-221019/765 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | a denial of service (DoS) condition. The vulnerability is due to improper management of system memory. An attacker could exploit this vulnerability by sending malicious IKEv1 traffic to an affected device. The attacker does not need valid credentials to authenticate the VPN session, nor does the attacker's source address need to match a peer statement in the crypto map applied to the ingress interface of the affected device. An exploit could allow the attacker to exhaust system memory resources, leading to a reload of an affected device.<br>**CVE ID : CVE-2019-15256** | | |
| **asa_5545-x** | | | | | |
| Uncontrolled Resource Consumption | 02-10-2019 | 7.8 | A vulnerability in the Internet Key Exchange version 1 (IKEv1) feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to improper management of system memory. An attacker could exploit this vulnerability by sending malicious IKEv1 traffic to an affected device. The attacker does not need valid credentials to | N/A | H-CIS-ASA_-221019/766 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | authenticate the VPN session, nor does the attacker's source address need to match a peer statement in the crypto map applied to the ingress interface of the affected device. An exploit could allow the attacker to exhaust system memory resources, leading to a reload of an affected device.<br>**CVE ID : CVE-2019-15256** | | |
| **compal** | | | | | |
| **ch7465lg** | | | | | |
| Improper Input Validation | 02-10-2019 | 7.5 | Compal CH7465LG CH7465LG-NCIP-6.12.18.24-5p8-NOSH devices have Incorrect Access Control because of Improper Input Validation. The attacker can send a maliciously modified POST (HTTP) request containing shell commands, which will be executed on the device, to an backend API endpoint of the cable modem.<br>**CVE ID : CVE-2019-13025** | N/A | H-COM-CH74-221019/767 |
| **fiberhome** | | | | | |
| **hg2201t** | | | | | |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 08-10-2019 | 5 | /var/WEB-GUI/cgi-bin/downloadfile.cgi on FiberHome HG2201T 1.00.M5007_JS_201804 devices allows pre-authentication Directory Traversal for reading arbitrary files.<br>**CVE ID : CVE-2019-17187** | N/A | H-FIB-HG22-221019/768 |
| **FON** | | | | | |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **fon2601e-se** | | | | | |
| Improper Input Validation | 04-10-2019 | 7.8 | FON2601E-SE, FON2601E-RE, FON2601E-FSW-S, and FON2601E-FSW-B with firmware versions 1.1.7 and earlier contain an issue where they may behave as open resolvers. If this vulnerability is exploited, FON routers may be leveraged for DNS amplification attacks to some other entities.<br>**CVE ID : CVE-2019-6015** | N/A | H-FON-FON2-221019/769 |
| **fon2601e-re** | | | | | |
| Improper Input Validation | 04-10-2019 | 7.8 | FON2601E-SE, FON2601E-RE, FON2601E-FSW-S, and FON2601E-FSW-B with firmware versions 1.1.7 and earlier contain an issue where they may behave as open resolvers. If this vulnerability is exploited, FON routers may be leveraged for DNS amplification attacks to some other entities.<br>**CVE ID : CVE-2019-6015** | N/A | H-FON-FON2-221019/770 |
| **fon2601e-fsw-s** | | | | | |
| Improper Input Validation | 04-10-2019 | 7.8 | FON2601E-SE, FON2601E-RE, FON2601E-FSW-S, and FON2601E-FSW-B with firmware versions 1.1.7 and earlier contain an issue where they may behave as open resolvers. If this vulnerability is exploited, FON routers may be leveraged for DNS amplification attacks to some other entities. | N/A | H-FON-FON2-221019/771 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID : CVE-2019-6015** | | |
| **fon2601e-fsw-b** | | | | | |
| Improper Input Validation | 04-10-2019 | 7.8 | FON2601E-SE, FON2601E-RE, FON2601E-FSW-S, and FON2601E-FSW-B with firmware versions 1.1.7 and earlier contain an issue where they may behave as open resolvers. If this vulnerability is exploited, FON routers may be leveraged for DNS amplification attacks to some other entities.<br>**CVE ID : CVE-2019-6015** | N/A | H-FON-FON2-221019/772 |
| **govicture** | | | | | |
| **pc530** | | | | | |
| Missing Authentication for Critical Function | 01-10-2019 | 10 | Victure PC530 devices allow unauthenticated TELNET access as root.<br>**CVE ID : CVE-2019-15940** | N/A | H-GOV-PC53-221019/773 |
| **socomec** | | | | | |
| **diris_a-40** | | | | | |
| Insufficiently Protected Credentials | 09-10-2019 | 10 | Password disclosure in the web interface on socomec DIRIS A-40 devices before 48250501 allows a remote attacker to get full access to a device via the /password.jsn URI.<br>**CVE ID : CVE-2019-15859** | N/A | H-SOC-DIRI-221019/774 |
| **vzug** | | | | | |
| **combi-stream_mslq** | | | | | |
| Improper Authentication | 06-10-2019 | 5 | An issue was discovered on V-Zug Combi-Steam MSLQ devices before Ethernet R07 and before WLAN R05. There | N/A | H-VZU-COMB-221019/775 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | is no bruteforce protection (e.g., lockout) established. An attacker might be able to bruteforce the password to authenticate on the device.<br>**CVE ID : CVE-2019-17215** | | |
| Improper Authenticati on | 06-10-2019 | 7.5 | An issue was discovered on V-Zug Combi-Steam MSLQ devices before Ethernet R07 and before WLAN R05. Password authentication uses MD5 to hash passwords. Cracking is possible with minimal effort.<br>**CVE ID : CVE-2019-17216** | N/A | H-VZU-COMB-221019/776 |
| Cross-Site Request Forgery (CSRF) | 06-10-2019 | 6.8 | An issue was discovered on V-Zug Combi-Steam MSLQ devices before Ethernet R07 and before WLAN R05. There is no CSRF protection established on the web service.<br>**CVE ID : CVE-2019-17217** | N/A | H-VZU-COMB-221019/777 |
| Missing Encryption of Sensitive Data | 06-10-2019 | 5 | An issue was discovered on V-Zug Combi-Steam MSLQ devices before Ethernet R07 and before WLAN R05. By default, the communication to the web service is unencrypted via http. An attacker is able to intercept and sniff communication to the web service.<br>**CVE ID : CVE-2019-17218** | N/A | H-VZU-COMB-221019/778 |
| Improper Authenticati on | 06-10-2019 | 5.8 | An issue was discovered on V-Zug Combi-Steam MSLQ devices before Ethernet R07 and before WLAN R05. By default, the device does not enforce any authentication. An | N/A | H-VZU-COMB-221019/779 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | adjacent attacker is able to use the network interface without proper access control.<br>**CVE ID : CVE-2019-17219** | | |
| **Xerox** | | | | | |
| **atlalink_b8045** | | | | | |
| Improper Privilege Management | 04-10-2019 | 7.5 | Xerox AtlaLink B8045/B8055/B8065/B8075/ B8090 C8030/C8035/C8045/C8055/ C8070 printers with software before 101.00x.089.22600 allow an attacker to gain privileges.<br>**CVE ID : CVE-2019-17184** | N/A | H-XER-ATLA-221019/780 |
| **atlalink_b8055** | | | | | |
| Improper Privilege Management | 04-10-2019 | 7.5 | Xerox AtlaLink B8045/B8055/B8065/B8075/ B8090 C8030/C8035/C8045/C8055/ C8070 printers with software before 101.00x.089.22600 allow an attacker to gain privileges.<br>**CVE ID : CVE-2019-17184** | N/A | H-XER-ATLA-221019/781 |
| **atlalink_b8065** | | | | | |
| Improper Privilege Management | 04-10-2019 | 7.5 | Xerox AtlaLink B8045/B8055/B8065/B8075/ B8090 C8030/C8035/C8045/C8055/ C8070 printers with software before 101.00x.089.22600 allow an attacker to gain privileges.<br>**CVE ID : CVE-2019-17184** | N/A | H-XER-ATLA-221019/782 |
| **atlalink_b8075** | | | | | |
| Improper | 04-10-2019 | 7.5 | Xerox AtlaLink | N/A | H-XER- |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Privilege Management | | | B8045/B8055/B8065/B8075/ B8090 C8030/C8035/C8045/C8055/ C8070 printers with software before 101.00x.089.22600 allow an attacker to gain privileges. **CVE ID : CVE-2019-17184** | | ATLA-221019/783 |
| **atlalink_b8090** | | | | | |
| Improper Privilege Management | 04-10-2019 | 7.5 | Xerox AtlaLink B8045/B8055/B8065/B8075/ B8090 C8030/C8035/C8045/C8055/ C8070 printers with software before 101.00x.089.22600 allow an attacker to gain privileges. **CVE ID : CVE-2019-17184** | N/A | H-XER-ATLA-221019/784 |
| **atlalink_c8030** | | | | | |
| Improper Privilege Management | 04-10-2019 | 7.5 | Xerox AtlaLink B8045/B8055/B8065/B8075/ B8090 C8030/C8035/C8045/C8055/ C8070 printers with software before 101.00x.089.22600 allow an attacker to gain privileges. **CVE ID : CVE-2019-17184** | N/A | H-XER-ATLA-221019/785 |
| **atlalink_c8035** | | | | | |
| Improper Privilege Management | 04-10-2019 | 7.5 | Xerox AtlaLink B8045/B8055/B8065/B8075/ B8090 C8030/C8035/C8045/C8055/ C8070 printers with software before 101.00x.089.22600 allow an attacker to gain privileges. **CVE ID : CVE-2019-17184** | N/A | H-XER-ATLA-221019/786 |

| Weakness | Publish Date | CVSS | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **atlalink_c8045** | | | | | |
| Improper Privilege Management | 04-10-2019 | 7.5 | Xerox AtlaLink B8045/B8055/B8065/B8075/ B8090 C8030/C8035/C8045/C8055/ C8070 printers with software before 101.00x.089.22600 allow an attacker to gain privileges.<br>**CVE ID : CVE-2019-17184** | N/A | H-XER-ATLA-221019/787 |
| **atlalink_c8055** | | | | | |
| Improper Privilege Management | 04-10-2019 | 7.5 | Xerox AtlaLink B8045/B8055/B8065/B8075/ B8090 C8030/C8035/C8045/C8055/ C8070 printers with software before 101.00x.089.22600 allow an attacker to gain privileges.<br>**CVE ID : CVE-2019-17184** | N/A | H-XER-ATLA-221019/788 |
| **atlalink_c8070** | | | | | |
| Improper Privilege Management | 04-10-2019 | 7.5 | Xerox AtlaLink B8045/B8055/B8065/B8075/ B8090 C8030/C8035/C8045/C8055/ C8070 printers with software before 101.00x.089.22600 allow an attacker to gain privileges.<br>**CVE ID : CVE-2019-17184** | N/A | H-XER-ATLA-221019/789 |