Release Notes for Cisco Cyber Vision Knowledge DB

Release 202109

Compatible device list

Center	Description
All version 4 centers	All Cisco Cyber Vision center version 4 are compatible with this Knowledge DB file.

Links

Software Download

The files listed below can be found using the following link:

https://software.cisco.com/download/home/286325414/type

Center	Description
CiscoCyberVision-center-4.0.1.ova	VMWare OVA file, for Center setup
CiscoCyberVision-center-4.0.1.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-center-with-DPI-4.0.1.ova	VMWare OVA file, for Center with DPI setup
CiscoCyberVision-sensor-management-4.0.1.ext	Sensor Management extension installation file
Sensor	**Description**
CiscoCyberVision-IOx-aarch64-4.0.1.tar	Cisco IE3400 and Cisco IR1101 installation and update file
CiscoCyberVision-IOx-IC3K-4.0.1.tar	Cisco IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-4.0.1.tar	Cisco Catalyst 9300 installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64-4.0.1.tar	Cisco IE3400 installation and update file, for Sensor with Active Discovery
CiscoCyberVision-IOx-Active-Discovery-x86-64-4.0.1.tar	Cisco Catalyst 9300 installation and update file, for Sensor with Active Discovery
Updates/4/4.0.1	**Description**
CiscoCyberVision-Embedded-KDB-4.0.1.dat	Knowledge DB embedded in Cisco Cyber Vision 4.0.1
Updates/KDB/KDB.202109	**Description**
CiscoCyberVision_knowledgedb_20210903.db	Knowledge DB version 20210903
CiscoCyberVision_knowledgedb_20210910.db	Knowledge DB version 20210910
CiscoCyberVision_knowledgedb_20210917.db	Knowledge DB version 20210917
CiscoCyberVision_knowledgedb_20210924.db	Knowledge DB version 20210924

Related Documentation

- Cisco Cyber Vision GUI User Guide:

  https://www.cisco.com/c/dam/en/us/td/docs/security/cyber_vision/Cisco_Cyber_Vision_GUI_User_Guide_4_0_0.pdf

Database download

Cisco Cyber Vision uses an internal database which contains the list of recognized vulnerabilities, icons, threats, etc. Cisco has published a new Knowledge DB for Cisco Cyber Vision. This Knowledge DB (or KDB) is essential for Cisco Cyber Vision. It allows, in particular, the detection of vulnerabilities.

This database can be updated using the file available from the link above. The file contains a built-in RSA signature and external checking is not required; the file will be verified by Cisco Cyber Vision Center at import time.

How to update the database

To update the Knowledge DB:

1. Download the latest DB file available.
2. From the Cisco Cyber Vision system administration page, click the Import a knowledge DB button to upload the file.

Importing the new database will rematch your existing components against any new vulnerabilities.

Release contents

20210924

This release includes additions to the Snort ruleset covering the following Talos advisories:

- **Talos Rules 2021-09-23 (https://www.snort.org/advisories/talos-rules-2021-09-23)**
  - Talos has added and modified multiple rules in the browser-ie, file-other, malware-cnc, malware-other, os-other, os-windows and server-other rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2021-09-21 (https://www.snort.org/advisories/talos-rules-2021-09-21)**
  - Talos has added and modified multiple rules in the indicator-shellcode, malware-cnc, malware-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2021-09-16 (https://www.snort.org/advisories/talos-rules-2021-09-16)**
  - Talos has added and modified multiple rules in the file-image, indicator-shellcode and os-windows rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2021-09-14 (https://www.snort.org/advisories/talos-rules-2021-09-14)**
  - Microsoft Vulnerability CVE-2021-36963: A coding deficiency exists in Microsoft Windows Common Log File System driver that may lead to an escalation of privilege.
  - Previously released rules will detect attacks targeting these vulnerabilities and have been updated with the appropriate reference information. They are also included in this release and are identified with GID 1, SIDs 40689 through 40690.
  - Microsoft Vulnerability CVE-2021-36975: A coding deficiency exists in Microsoft Win32k that may lead to an escalation of privilege.
  - Rules to detect attacks targeting these vulnerabilities are included in this release and are identified with GID 1, SIDs 58136 through 58137.
  - Microsoft Vulnerability CVE-2021-38633: A coding deficiency exists in Microsoft Windows Common Log File System driver that may lead to an escalation of privilege.
  - Rules to detect attacks targeting these vulnerabilities are included in this release and are identified with GID 1, SIDs 58140 through 58141.
  - Microsoft Vulnerability CVE-2021-40444: A coding deficiency exists in Microsoft MSHTML Engine that may lead to remote code execution.
  - Previously released rules will detect attacks targeting these vulnerabilities and have been updated with the appropriate reference information. They are also included in this release and are identified with GID 1, SIDs 58120 through 58129 and 58132 through 58135.
  - Talos also has added and modified multiple rules in the file-image, file-other, malware-other, os-windows and server-webapp rule sets to provide coverage for emerging threats from these technologies.

This release also adds support and modifications for the detection of the following vulnerabilities:

- CVE-2021-34768: (Cisco IOS XE Software for Catalyst 9000 Family Wireless Controllers CAPWAP Denial of Service Vulnerabilities)

  Multiple vulnerabilities in the Control and Provisioning of Wireless Access Points (CAPWAP) protocol processing of Cisco IOS XE Software for Cisco Catalyst 9000 Family Wireless Controllers could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. These vulnerabilities are due to insufficient validation of CAPWAP packets. An attacker could exploit the vulnerabilities by sending a malformed CAPWAP packet to an affected device. A successful exploit could allow the attacker to cause the affected device to crash and reload, resulting in a DoS condition.

- CVE-2021-1616: (Cisco IOS XE Software H.323 Application Level Gateway Bypass Vulnerability)

  A vulnerability in the H.323 application level gateway (ALG) used by the Network Address Translation (NAT) feature of Cisco IOS XE Software could allow an unauthenticated, remote attacker to bypass the ALG. This vulnerability is due to insufficient data validation of traffic that is traversing the ALG. An attacker could exploit this vulnerability by sending crafted traffic to a targeted device. A successful exploit could allow the attacker to bypass the ALG and open connections that should not be allowed to a remote device located behind the ALG. Note: This vulnerability has been publicly discussed as NAT Slipstreaming.

- CVE-2021-34696: (Cisco ASR 900 and ASR 920 Series Aggregation Services Routers Access Control List Bypass Vulnerability)

  A vulnerability in the access control list (ACL) programming of Cisco ASR 900 and ASR 920 Series Aggregation Services Routers could allow an unauthenticated, remote attacker to bypass a configured ACL. This vulnerability is due to incorrect programming of hardware when an ACL is configured using a method other than the configuration CLI. An attacker could exploit this vulnerability by attempting to send traffic through an affected device. A successful exploit could allow the attacker to bypass an ACL on the affected device.

- CVE-2021-34767: (Cisco IOS XE Software for Catalyst 9800 Series Wireless Controllers IPv6 Denial of Service Vulnerability)

  A vulnerability in IPv6 traffic processing of Cisco IOS XE Wireless Controller Software for Cisco Catalyst 9000 Family Wireless Controllers could allow an unauthenticated, adjacent attacker to cause a Layer 2 (L2) loop in a configured VLAN, resulting in a denial of service (DoS) condition for that VLAN. The vulnerability is due to a logic error when processing specific link-local IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that would flow inbound through the wired interface of an affected device. A successful exploit could allow the attacker to cause traffic drops in the affected VLAN, thus triggering the DoS condition.

- CVE-2021-34714: (Multiple Cisco Operating Systems Unidirectional Link Detection Denial of Service Vulnerability)

  A vulnerability in the Unidirectional Link Detection (UDLD) feature of Cisco FXOS Software, Cisco IOS Software, Cisco IOS XE Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause an affected device to reload. This vulnerability is due to improper input validation of the UDLD packets. An attacker could exploit this vulnerability by sending specifically crafted UDLD packets to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a denial of service (DoS) condition. Note: The UDLD feature is disabled by default, and the conditions to exploit this vulnerability are strict. An attacker must have full control of a directly connected device. On Cisco IOS XR devices, the impact is limited to the reload of the UDLD process.

- CVE-2021-1622: (Cisco IOS XE Software for Cisco cBR-8 Converged Broadband Routers Common Open Policy Service Denial of Service Vulnerability)

  A vulnerability in the Common Open Policy Service (COPS) of Cisco IOS XE Software for Cisco cBR-8 Converged Broadband Routers could allow an unauthenticated, remote attacker to cause resource

exhaustion, resulting in a denial of service (DoS) condition. This vulnerability is due to a deadlock condition in the code when processing COPS packets under certain conditions. An attacker could exploit this vulnerability by sending COPS packets with high burst rates to an affected device. A successful exploit could allow the attacker to cause the CPU to consume excessive resources, which prevents other control plane processes from obtaining resources and results in a DoS.

- CVE-2021-1621: (Cisco IOS XE Software Interface Queue Wedge Denial of Service Vulnerability)
  A vulnerability in the Layer 2 punt code of Cisco IOS XE Software could allow an unauthenticated, adjacent attacker to cause a queue wedge on an interface that receives specific Layer 2 frames, resulting in a denial of service (DoS) condition. This vulnerability is due to improper handling of certain Layer 2 frames. An attacker could exploit this vulnerability by sending specific Layer 2 frames on the segment the router is connected to. A successful exploit could allow the attacker to cause a queue wedge on the interface, resulting in a DoS condition.
- CVE-2021-34770: (Cisco IOS XE Software for Catalyst 9000 Family Wireless Controllers CAPWAP Remote Code Execution Vulnerability)
  A vulnerability in the Control and Provisioning of Wireless Access Points (CAPWAP) protocol processing of Cisco IOS XE Software for Cisco Catalyst 9000 Family Wireless Controllers could allow an unauthenticated, remote attacker to execute arbitrary code with administrative privileges or cause a denial of service (DoS) condition on an affected device. The vulnerability is due to a logic error that occurs during the validation of CAPWAP packets. An attacker could exploit this vulnerability by sending a crafted CAPWAP packet to an affected device. A successful exploit could allow the attacker to execute arbitrary code with administrative privileges or cause the affected device to crash and reload, resulting in a DoS condition.
- CVE-2021-1623: (Cisco IOS XE Software for Cisco cBR-8 Converged Broadband Routers Simple Network Management Protocol Denial of Service Vulnerability)
  A vulnerability in the Simple Network Management Protocol (SNMP) punt handling function of Cisco cBR-8 Converged Broadband Routers could allow an authenticated, remote attacker to overload a device punt path, resulting in a denial of service (DoS) condition. This vulnerability is due to the punt path being overwhelmed by large quantities of SNMP requests. An attacker could exploit this vulnerability by sending a large number of SNMP requests to an affected device. A successful exploit could allow the attacker to overload the device punt path, resulting in a DoS condition.
- CVE-2021-1624: (Cisco IOS XE Software Rate Limiting Network Address Translation Denial of Service Vulnerability)
  A vulnerability in the Rate Limiting Network Address Translation (NAT) feature of Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause high CPU utilization in the Cisco QuantumFlow Processor of an affected device, resulting in a denial of service (DoS) condition. This vulnerability is due to mishandling of the rate limiting feature within the QuantumFlow Processor. An attacker could exploit this vulnerability by sending large amounts of traffic that would be subject to NAT and rate limiting through an affected device. A successful exploit could allow the attacker to cause the QuantumFlow Processor utilization to reach 100 percent on the affected device, resulting in a DoS condition.
- CVE-2021-34769: (Cisco IOS XE Software for Catalyst 9000 Family Wireless Controllers CAPWAP Denial of Service Vulnerabilities)
  Multiple vulnerabilities in the Control and Provisioning of Wireless Access Points (CAPWAP) protocol processing of Cisco IOS XE Software for Cisco Catalyst 9000 Family Wireless Controllers could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. These vulnerabilities are due to insufficient validation of CAPWAP packets. An attacker could exploit the vulnerabilities by sending a malformed CAPWAP packet to an affected device. A successful exploit could allow the attacker to cause the affected device to crash and reload, resulting in a DoS condition.

- CVE-2021-1611: (Cisco IOS XE Software for Catalyst 9800 Series Wireless Controllers EoGRE Denial of Service Vulnerability)
  A vulnerability in Ethernet over GRE (EoGRE) packet processing of Cisco IOS XE Wireless Controller Software for the Cisco Catalyst 9800 Family Wireless Controller, Embedded Wireless Controller, and Embedded Wireless on Catalyst 9000 Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper processing of malformed EoGRE packets. An attacker could exploit this vulnerability by sending malicious packets to the affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition.
- CVE-2021-1615: (Cisco Embedded Wireless Controller Software for Catalyst Access Points Denial of Service Vulnerability)
  A vulnerability in the packet processing functionality of Cisco Embedded Wireless Controller (EWC) Software for Catalyst Access Points (APs) could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected AP. This vulnerability is due to insufficient buffer allocation. An attacker could exploit this vulnerability by sending crafted traffic to an affected device. A successful exploit could allow the attacker to exhaust available resources and cause a DoS condition on an affected AP, as well as a DoS condition for client traffic traversing the AP.
- CVE-2021-34699: (Cisco IOS and IOS XE Software TrustSec CLI Parser Denial of Service Vulnerability)
  A vulnerability in the TrustSec CLI parser of Cisco IOS and Cisco IOS XE Software could allow an authenticated, remote attacker to cause an affected device to reload. This vulnerability is due to an improper interaction between the web UI and the CLI parser. An attacker could exploit this vulnerability by requesting a particular CLI command to be run through the web UI. A successful exploit could allow the attacker to cause the device to reload, resulting in a denial of service (DoS) condition.
- CVE-2021-1620: (Cisco IOS and IOS XE Software IKEv2 AutoReconnect Feature Denial of Service Vulnerability)
  A vulnerability in the Internet Key Exchange Version 2 (IKEv2) support for the AutoReconnect feature of Cisco IOS Software and Cisco IOS XE Software could allow an authenticated, remote attacker to exhaust the free IP addresses from the assigned local pool. This vulnerability occurs because the code does not release the allocated IP address under certain failure conditions. An attacker could exploit this vulnerability by trying to connect to the device with a non-AnyConnect client. A successful exploit could allow the attacker to exhaust the IP addresses from the assigned local pool, which prevents users from logging in and leads to a denial of service (DoS) condition.
- CVE-2021-34723: (Cisco IOS XE SD-WAN Software Arbitrary File Overwrite Vulnerability)
  A vulnerability in a specific CLI command that is run on Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to overwrite arbitrary files in the configuration database of an affected device. This vulnerability is due to insufficient validation of specific CLI command parameters. An attacker could exploit this vulnerability by issuing that command with specific parameters. A successful exploit could allow the attacker to overwrite the content of the configuration database and gain root-level access to an affected device.
- CVE-2021-34703: (Cisco IOS and IOS XE Software Link Layer Discovery Protocol Denial of Service Vulnerability)
  A vulnerability in the Link Layer Discovery Protocol (LLDP) message parser of Cisco IOS Software and Cisco IOS XE Software could allow an attacker to trigger a reload of an affected device, resulting in a denial of service (DoS) condition. This vulnerability is due to improper initialization of a buffer. An attacker could exploit this vulnerability via any of the following methods: An authenticated, remote attacker could access the LLDP neighbor table via either the CLI or SNMP while the device is in a specific state. An unauthenticated, adjacent attacker could corrupt the LLDP neighbor table by injecting specific LLDP frames into the network and then waiting for an administrator of the device or a network management system (NMS) managing the device to retrieve the LLDP neighbor table of the device via either the CLI or SNMP.

An authenticated, adjacent attacker with SNMP read-only credentials or low privileges on the device CLI could corrupt the LLDP neighbor table by injecting specific LLDP frames into the network and then accessing the LLDP neighbor table via either the CLI or SNMP. A successful exploit could allow the attacker to cause the affected device to crash, resulting in a reload of the device.

- CVE-2021-34697: (Cisco IOS XE Software Protection Against Distributed Denial of Service Attacks Feature Vulnerability)
  A vulnerability in the Protection Against Distributed Denial of Service Attacks feature of Cisco IOS XE Software could allow an unauthenticated, remote attacker to conduct denial of service (DoS) attacks to or through the affected device. This vulnerability is due to incorrect programming of the half-opened connections limit, TCP SYN flood limit, or TCP SYN cookie features when the features are configured in vulnerable releases of Cisco IOS XE Software. An attacker could exploit this vulnerability by attempting to flood traffic to or through the affected device. A successful exploit could allow the attacker to initiate a DoS attack to or through an affected device.
- CVE-2021-34705: (Cisco IOS and IOS XE Software FXO Interface Destination Pattern Bypass Vulnerability)
  A vulnerability in the Voice Telephony Service Provider (VTSP) service of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to bypass configured destination patterns and dial arbitrary numbers. This vulnerability is due to insufficient validation of dial strings at Foreign Exchange Office (FXO) interfaces. An attacker could exploit this vulnerability by sending a malformed dial string to an affected device via either the ISDN protocol or SIP. A successful exploit could allow the attacker to conduct toll fraud, resulting in unexpected financial impact to affected customers.
- CVE-2021-1619: (Cisco IOS XE Software NETCONF and RESTCONF Authentication Bypass Vulnerability)
  A vulnerability in the authentication, authorization, and accounting (AAA) function of Cisco IOS XE Software could allow an unauthenticated, remote attacker to bypass NETCONF or RESTCONF authentication and do either of the following: Install, manipulate, or delete the configuration of an affected device Cause memory corruption that results in a denial of service (DoS) on an affected device This vulnerability is due to an uninitialized variable. An attacker could exploit this vulnerability by sending a series of NETCONF or RESTCONF requests to an affected device. A successful exploit could allow the attacker to use NETCONF or RESTCONF to install, manipulate, or delete the configuration of a network device or to corrupt memory on the device, resulting a DoS.
- CVE-2021-1625: (Cisco IOS XE Software Zone-Based Policy Firewall ICMP and UDP Inspection Vulnerability)
  A vulnerability in the Zone-Based Policy Firewall feature of Cisco IOS XE Software could allow an unauthenticated, remote attacker to prevent the Zone-Based Policy Firewall from correctly classifying traffic. This vulnerability exists because ICMP and UDP responder-to-initiator flows are not inspected when the Zone-Based Policy Firewall has either Unified Threat Defense (UTD) or Application Quality of Experience (AppQoE) configured. An attacker could exploit this vulnerability by attempting to send UDP or ICMP flows through the network. A successful exploit could allow the attacker to inject traffic through the Zone-Based Policy Firewall, resulting in traffic being dropped because it is incorrectly classified or in incorrect reporting figures being produced by high-speed logging (HSL).
- CVE-2021-1565: (Cisco IOS XE Software for Catalyst 9000 Family Wireless Controllers CAPWAP Denial of Service Vulnerabilities)
  Multiple vulnerabilities in the Control and Provisioning of Wireless Access Points (CAPWAP) protocol processing of Cisco IOS XE Software for Cisco Catalyst 9000 Family Wireless Controllers could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. These vulnerabilities are due to insufficient validation of CAPWAP packets. An attacker could exploit the vulnerabilities by sending a malformed CAPWAP packet to an affected device. A successful exploit could allow the attacker to cause the affected device to crash and reload, resulting in a DoS condition.

20210917

This release includes additions to the Snort ruleset covering the following Talos advisories:

- **Talos Rules 2021-09-10 (https://www.snort.org/advisories/talos-rules-2021-09-10)**
  - Talos is releasing enhanced coverage for CVE-2021-40444 in SIDs 58130-58135.
  - Talos has added and modified multiple rules in the file-office rule sets to provide coverage for emerging threats from these technologies.

This release also adds support and modifications for the detection of the following vulnerabilities:

- CVE-2021-33824: (Denial-of-service Vulnerability in Moxa MGate MB3180/MB3280/MB3480 Series)
  An attacker could perform a denial-of-service attack by sending incomplete packets to exhaust the web servers' resources.
- CVE-2021-33823: (Denial-of-service Vulnerability in Moxa MGate MB3180/MB3280/MB3480 Series)
  An attacker could perform a denial-of-service attack by flooding the device with packets and exhausting the web servers' resources.
- CVE-2021-22798: (Insufficiently Protected Credentials vulnerability in Conext ComBox)
  A CWE-522: Insufficiently Protected Credentials vulnerability exists that could cause Sensitive data such as login credentials being exposed when a Network is sniffed.
- CVE-2021-22788: (Out-of-bounds Write vulnerability in Web Server on Modicon M340, Legacy Offers Modicon Quantum and Premium and Associated Communication Modules)
  A CWE-787: Out-of-bounds Write vulnerability exists that could cause denial of service when an attacker sends a specially crafted HTTP request to the web server of the device.
- CVE-2021-22787: (Improper Input Validation vulnerability in Web Server on Modicon M340, Legacy Offers Modicon Quantum and Premium and Associated Communication Modules)
  A CWE-20: Improper Input Validation vulnerability exists that could cause denial of service of the device when an attacker sends a specially crafted HTTP request to the web server of the device.
- CVE-2021-22785: (Information Exposure vulnerability in Web Server on Modicon M340, Legacy Offers Modicon Quantum and Premium and Associated Communication Modules)
  A CWE-200: Information Exposure vulnerability exists that could cause sensitive information of files located in the web root directory to leak when an attacker sends a HTTP request to the web server of the device.
- CVE-2021-37175: (Improper Handling of Insufficient Permissions or Privileges Vulnerability in Siemens RUGGEDCOM ROX)
  The affected devices do not properly handle permissions to traverse the file system. If exploited, an attacker could gain access to an overview of the overview of the complete file system on the affected devices.
- CVE-2021-33720: (Classic Buffer Overflow Vulnerability in Siemens SIPROTEC 5 relays)
  An attacker can send specially crafted packets to Port 4443/TCP, which may cause a denial-of-service condition.
- CVE-2021-37173: (Exposure of Sensitive Information to an Unauthorized Actor Vulnerability in Siemens RUGGEDCOM ROX)
  The affected devices have an exposure of sensitive information vulnerability that could allow an authenticated attacker to extract data via Secure Shell (SSH).
- CVE-2021-37206: (Improper Input Validation Vulnerability in Siemens SIPROTEC 5)

Received web packets are not properly processed. An unauthenticated remote attacker with access to any of the Ethernet interfaces could send specially crafted packets to force a restart of the target device.

- CVE-2021-33716: (Cleartext Storage of Sensitive Information Vulnerability in Siemens SIMATIC CP 1543-1 (incl. SIPLUS variants) and SIMATIC CP 1545-1)
  An attacker with access to the subnet of the affected device could retrieve sensitive information stored in cleartext.
- CVE-2020-28397: (Incorrect Authorization Vulnerability in Siemens SIMATIC and TIM)
  The affected products are vulnerable to an incorrect authorization check, allowing an attacker to extract information about access protected PLC program variables when simultaneously reading multiple attributes.
- CVE-2021-33737: (Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability in Siemens SIMATIC CP)
  Sending a specially crafted packet to Port 102/TCP of an affected device could cause a denial-of-service condition. A restart is needed to restore normal operations.
- CVE-2021-27391: (Classic Buffer Overflow Vulnerability in Siemens APOGEE and TALON)
  The web server of affected devices lacks proper bounds checking when parsing specific requests, which could lead to a buffer overflow. An unauthenticated remote attacker could exploit this vulnerability to execute arbitrary code on the device with root privileges.
- CVE-2021-37186: (Use of Insufficiently Random Values Vulnerability in Siemens Devices)
  The underlying TCP/IP stack does not properly calculate the random numbers used as ISN (Initial Sequence Numbers). An adjacent attacker with network access to the LAN interface could interfere with traffic, spoof the connection, and gain access to sensitive information.
- CVE-2021-33719: (Classic Buffer Overflow Vulnerability in Siemens SIPROTEC 5 relays)
  An attacker can send specially crafted packets to Port 4443/TCP, which may cause a denial-of-service condition or a remote code execution.
- CVE-2020-36475: (Improper Certificate Validation Vulnerability in Siemens LOGO! and SIMATIC RTU 3000 family)
  The calculations performed in the third-party component Mbed TLS are not limited. Supplying overly large parameters could lead to denial-of-service condition when generating Diffie-Hellman key pairs.
- CVE-2020-7461: (Out-of-bounds Write Vulnerability in Siemens SIMATIC RFID terminals)
  In FreeBSD 12.1-STABLE before r365010, 11.4-STABLE before r365011, 12.1-RELEASE before p9, 11.4-RELEASE before p3, and 11.3-RELEASE before p13, dhclient(8) fails to handle certain malformed input related to handling of DHCP option 119, resulting a heap overflow. The heap overflow could be exploited to achieve remote code execution. The affected process runs with reduced privileges in a Capsicum sandbox, limiting the immediate impact of an exploit.
- CVE-2020-36478: (Incorrect Calculation of Buffer Size Vulnerability in Siemens LOGO! and SIMATIC RTU 3000 family)
  The affected product is vulnerable to a stack-based buffer overflow, which may allow an attacker to remotely execute arbitrary code.
- CVE-2021-37174: (Execution with Unnecessary Privileges Vulnerability in Siemens RUGGEDCOM ROX)
  The affected devices have a privilege escalation vulnerability that could allow an attacker to gain root user access.

20210910

This release includes additions to the Snort ruleset covering the following Talos advisories:

- **Talos Rules 2021-09-09 (https://www.snort.org/advisories/talos-rules-2021-09-09)**
  - Today Talos is releasing coverage to detect exploitation attempts of Microsoft Office ActiveX control abuse, designated under CVE-2021-40444. Coverage is being released as SIDs 58120-58129 and native Snort 3 SID 300049. Talos may release additional coverage in the future as the situation develops and new guidance is created.
  - Talos has added and modified multiple rules in the file-office, malware-cnc, os-windows and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2021-09-07 (https://www.snort.org/advisories/talos-rules-2021-09-07)**
  - Talos has added and modified multiple rules in the browser-chrome and malware-other rule sets to provide coverage for emerging threats from these technologies.

This release also adds support and modifications for the detection of the following vulnerabilities:

- CVE-2021-34771: (Cisco IOS XR Software Unauthorized Information Disclosure Vulnerability)
  A vulnerability in the Cisco IOS XR Software CLI could allow an authenticated, local attacker to view more information than their privileges allow. This vulnerability is due to insufficient application of restrictions during the execution of a specific command. An attacker could exploit this vulnerability by running a specific command. A successful exploit could allow the attacker to view sensitive configuration information that their privileges might not otherwise allow them to access.
- CVE-2021-34728: (Cisco IOS XR Software Authenticated User Privilege Escalation Vulnerabilities)
  Multiple vulnerabilities in the CLI of Cisco IOS XR Software could allow an authenticated, local attacker with a low-privileged account to elevate privileges on an affected device.
- CVE-2021-1588: (Cisco NX-OS Software MPLS OAM Denial of Service Vulnerability)
  A vulnerability in the MPLS Operation, Administration, and Maintenance (OAM) feature of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper input validation when an affected device is processing an MPLS echo-request or echo-reply packet. An attacker could exploit this vulnerability by sending malicious MPLS echo-request or echo-reply packets to an interface that is enabled for MPLS forwarding on the affected device. A successful exploit could allow the attacker to cause the MPLS OAM process to crash and restart multiple times, causing the affected device to reload and resulting in a DoS condition.
- CVE-2021-34720: (Cisco IOS XR Software IP Service Level Agreements and Two-Way Active Measurement Protocol Denial of Service Vulnerability)
  A vulnerability in the IP Service Level Agreements (IP SLA) responder and Two-Way Active Measurement Protocol (TWAMP) features of Cisco IOS XR Software could allow an unauthenticated, remote attacker to cause device packet memory to become exhausted or cause the IP SLA process to crash, resulting in a denial of service (DoS) condition. This vulnerability exists because socket creation failures are mishandled during the IP SLA and TWAMP processes. An attacker could exploit this vulnerability by sending specific IP SLA or TWAMP packets to an affected device. A successful exploit could allow the attacker to exhaust the packet memory, which will impact other processes, such as routing protocols, or crash the IP SLA process.
- CVE-2021-1440: (Cisco IOS XR Software Border Gateway Protocol Resource Public Key Infrastructure Denial of Service Vulnerability)
  A vulnerability in the implementation of the Resource Public Key Infrastructure (RPKI) feature of Cisco IOS XR Software could allow an unauthenticated, remote attacker to cause the Border Gateway Protocol (BGP)

process to crash, resulting in a denial of service (DoS) condition. This vulnerability is due to the incorrect handling of a specific RPKI to Router (RTR) Protocol packet header. An attacker could exploit this vulnerability by compromising the RPKI validator server and sending a specifically crafted RTR packet to an affected device. Alternatively, the attacker could use man-in-the-middle techniques to impersonate the RPKI validator server and send a specifically crafted RTR response packet over the established RTR TCP connection to the affected device. A successful exploit could allow the attacker to cause a DoS condition because the BGP process could constantly restart and BGP routing could become unstable.

- CVE-2021-34719: (Cisco IOS XR Software Authenticated User Privilege Escalation Vulnerabilities)
  Multiple vulnerabilities in the CLI of Cisco IOS XR Software could allow an authenticated, local attacker with a low-privileged account to elevate privileges on an affected device.
- CVE-2021-34737: (Cisco IOS XR Software DHCP Version 4 Server Denial of Service Vulnerability)
  A vulnerability in the DHCP version 4 (DHCPv4) server feature of Cisco IOS XR Software could allow an unauthenticated, remote attacker to trigger a crash of the dhcpd process, resulting in a denial of service (DoS) condition. This vulnerability exists because certain DHCPv4 messages are improperly validated when they are processed by an affected device. An attacker could exploit this vulnerability by sending a malformed DHCPv4 message to an affected device. A successful exploit could allow the attacker to cause a NULL pointer dereference, resulting in a crash of the dhcpd process. While the dhcpd process is restarting, which may take up to approximately two minutes, DHCPv4 server services are unavailable on the affected device. This could temporarily prevent network access to clients that join the network during that time period. Note: Only the dhcpd process crashes and eventually restarts automatically. The router does not reload.
- CVE-2021-34718: (Cisco IOS XR Software Arbitrary File Read and Write Vulnerability)
  A vulnerability in the SSH Server process of Cisco IOS XR Software could allow an authenticated, remote attacker to overwrite and read arbitrary files on the local device. This vulnerability is due to insufficient input validation of arguments that are supplied by the user for a specific file transfer method. An attacker with lower-level privileges could exploit this vulnerability by specifying Secure Copy Protocol (SCP) parameters when authenticating to a device. A successful exploit could allow the attacker to elevate their privileges and retrieve and upload files on a device that they should not have access to.
- CVE-2021-1587: (Cisco NX-OS Software VXLAN OAM (NGOAM) Denial of Service Vulnerability)
  A vulnerability in the VXLAN Operation, Administration, and Maintenance (OAM) feature of Cisco NX-OS Software, known as NGOAM, could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper handling of specific packets with a Transparent Interconnection of Lots of Links (TRILL) OAM EtherType. An attacker could exploit this vulnerability by sending crafted packets, including the TRILL OAM EtherType of 0x8902, to a device that is part of a VXLAN Ethernet VPN (EVPN) fabric. A successful exploit could allow the attacker to cause an affected device to experience high CPU usage and consume excessive system resources, which may result in overall control plane instability and cause the affected device to reload. Note: The NGOAM feature is disabled by default.
- CVE-2021-34708: (Cisco IOS XR Software for Cisco 8000 and Network Convergence System 540 Series Routers Image Verification Vulnerabilities)
  Multiple vulnerabilities in image verification checks of Cisco Network Convergence System (NCS) 540 Series Routers, only when running Cisco IOS XR NCS540L software images, and Cisco IOS XR Software for Cisco 8000 Series Routers could allow an authenticated, local attacker to execute arbitrary code on the underlying operating system.
- CVE-2021-34722: (Cisco IOS XR Software Command Injection Vulnerabilities)
  Multiple vulnerabilities in the CLI of Cisco IOS XR Software could allow an authenticated, local attacker to

gain access to the underlying root shell of an affected device and execute arbitrary commands with root privileges.

- CVE-2021-1591: (Cisco Nexus 9500 Series Switches Access Control List Bypass Vulnerability)
  A vulnerability in the EtherChannel port subscription logic of Cisco Nexus 9500 Series Switches could allow an unauthenticated, remote attacker to bypass access control list (ACL) rules that are configured on an affected device. This vulnerability is due to oversubscription of resources that occurs when applying ACLs to port channel interfaces. An attacker could exploit this vulnerability by attempting to access network resources that are protected by the ACL. A successful exploit could allow the attacker to access network resources that would be protected by the ACL that was applied on the port channel interface.
- CVE-2021-34709: (Cisco IOS XR Software for Cisco 8000 and Network Convergence System 540 Series Routers Image Verification Vulnerabilities)
  Multiple vulnerabilities in image verification checks of Cisco Network Convergence System (NCS) 540 Series Routers, only when running Cisco IOS XR NCS540L software images, and Cisco IOS XR Software for Cisco 8000 Series Routers could allow an authenticated, local attacker to execute arbitrary code on the underlying operating system.
- CVE-2021-1590: (Cisco NX-OS Software system login block-for Denial of Service Vulnerability)
  A vulnerability in the implementation of the system login block-for command for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a login process to unexpectedly restart, causing a denial of service (DoS) condition. This vulnerability is due to a logic error in the implementation of the system login block-for command when an attack is detected and acted upon. An attacker could exploit this vulnerability by performing a brute-force login attack on an affected device. A successful exploit could allow the attacker to cause a login process to reload, which could result in a delay during authentication to the affected device.
- CVE-2021-34721: (Cisco IOS XR Software Command Injection Vulnerabilities)
  Multiple vulnerabilities in the CLI of Cisco IOS XR Software could allow an authenticated, local attacker to gain access to the underlying root shell of an affected device and execute arbitrary commands with root privileges.
- CVE-2021-34713: (Cisco IOS XR Software for ASR 9000 Series Routers Denial of Service Vulnerability)
  A vulnerability in the Layer 2 punt code of Cisco IOS XR Software running on Cisco ASR 9000 Series Aggregation Services Routers could allow an unauthenticated, adjacent attacker to cause the affected line card to reboot. This vulnerability is due to incorrect handling of specific Ethernet frames that cause a spin loop that can make the network processors unresponsive. An attacker could exploit this vulnerability by sending specific types of Ethernet frames on the segment where the affected line cards are attached. A successful exploit could allow the attacker to cause the affected line card to reboot.

20210903

This release includes additions to the Snort ruleset covering the following Talos advisories:

- **Talos Rules 2021-09-02 (https://www.snort.org/advisories/talos-rules-2021-09-02)**
  - Talos has added and modified multiple rules in the browser-chrome, browser-ie, browser-other, browser-webkit, deleted, exploit-kit, file-executable, file-flash, file-image, file-java, file-multimedia, file-office, file-other, file-pdf, indicator-compromise, indicator-shellcode, malware-cnc, malware-other, netbios, os-linux, os-other, os-windows, policy-other, policy-social, protocol-dns, protocol-icmp, protocol-nntp, protocol-other, protocol-scada, protocol-snmp, protocol-tftp, protocol-voip, pua-p2p, server-iis, server-mail, server-mysql, server-oracle, server-other and server-webapp rule sets to provide

coverage for emerging threats from these technologies.

- **Talos Rules 2021-08-31 (https://www.snort.org/advisories/talos-rules-2021-08-31)**
  - Talos has added and modified multiple rules in the browser-ie, file-image and server-webapp rule sets to provide coverage for emerging threats from these technologies.

This release also adds support and modifications for the detection of the following vulnerabilities:

- CVE-2021-39278: (Reflected Cross-site scripting via manipulated config-file)
  Allows an attacker to import a malicious config file to the device through the web interface.
- CVE-2021-39279: (Authenticated Command Injection in Moxa devices)
  A specially crafted command can cause privilege escalation and circumvent the operating system's user access controls.
- CVE-2016-2148: (busybox: Improper Restriction of Operations within the Bounds of a Memory Buffer)
  Heap-based buffer overflow in the DHCP client (udhcpc) in BusyBox before 1.25.0 allows remote attackers to have unspecified impact via vectors involving OPTION_6RD parsing.
- CVE-2016-7406: (dropbear ssh: Improper Input Validation)
  Format string vulnerability in Dropbear SSH before 2016.74 allows remote attackers to execute arbitrary code via format string specifiers in the (1) username or (2) host argument.
- CVE-2012-4412: (glibc: Numeric Errors)
  Integer overflow in string/strcoll_l.c in the GNU C Library (aka glibc or libc6) 2.17 and earlier allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a long string, which triggers a heap-based buffer overflow.
- CVE-2014-5119: (glibc: Numeric Errors)
  Off-by-one error in the __gconv_translit_find function in gconv_trans.c in GNU C Library (aka glibc) allows context-dependent attackers to cause a denial of service (crash) or execute arbitrary code via vectors related to the CHARSET environment variable and gconv transliteration modules.
- CVE-2014-9402: (glibc: Resource Management Errors)
  The nss_dns implementation of getnetbyname in GNU C Library (aka glibc) before 2.21, when the DNS backend in the Name Service Switch configuration is enabled, allows remote attackers to cause a denial of service (infinite loop) by sending a positive answer while a network name is being process.
- CVE-2014-9984: (glibc: Improper Restriction of Operations within the Bounds of a Memory Buffer)
  nscd in the GNU C Library (aka glibc or libc6) before version 2.20 does not correctly compute the size of an internal buffer when processing netgroup requests, possibly leading to an nscd daemon crash or code execution as the user running nscd.
- CVE-2018-6485: (glibc: Multiple vulnerabilities including Out-of-bounds Write, Integer Overflow or Wraparound)
  An integer overflow in the implementation of the posix_memalign in memalign functions in the GNU C Library (aka glibc or libc6) 2.26 and earlier could cause these functions to return a pointer to a heap area that is too small, potentially leading to heap corruption.
- CVE-2015-7547: (glibc: Improper Restriction of Operations within the Bounds of a Memory Buffer)
  Multiple stack-based buffer overflows in the (1) send_dg and (2) send_vc functions in the libresolv library in the GNU C Library (aka glibc or libc6) before 2.23 allow remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted DNS response that triggers a call to the getaddrinfo function with the AF_UNSPEC or AF_INET6 address family, related to performing "dual A/AAAA DNS queries" and the libnss_dns.so.2 NSS module.

- CVE-2015-0235: (glibc: Out-of-bounds Write)
  Heap-based buffer overflow in the __nss_hostname_digits_dots function in glibc 2.2, and other 2.x versions before 2.18, allows context-dependent attackers to execute arbitrary code via vectors related to the (1) gethostbyname or (2) gethostbyname2 function, aka "GHOST."
- CVE-2008-4609: (TCP protocol implementation: Multiple vulnerabilities including Insufficient Information, Configuration)
  The TCP implementation in (1) Linux, (2) platforms based on BSD Unix, (3) Microsoft Windows, (4) Cisco products, and probably other operating systems allows remote attackers to cause a denial of service (connection queue exhaustion) via multiple vectors that manipulate information in the TCP state table, as demonstrated by sockstress.
- CVE-2009-1298: (linux kernel: Improper Restriction of Operations within the Bounds of a Memory Buffer)
  The ip_frag_reasm function in net/ipv4/ip_fragment.c in the Linux kernel 2.6.32-rc8, and 2.6.29 and later versions before 2.6.32, calls IP_INC_STATS_BH with an incorrect argument, which allows remote attackers to cause a denial of service (NULL pointer dereference and hang) via long IP packets, possibly related to the ip_defrag function.
- CVE-2010-1162: (linux kernel: memory leak, possibly resulting in a denial of service)
  The release_one_tty function in drivers/char/tty_io.c in the Linux kernel before 2.6.34-rc4 omits certain required calls to the put_pid function, which has unspecified impact and local attack vectors.
- CVE-2010-4251: (linux kernel: Uncontrolled Resource Consumption)
  The socket implementation in net/core/sock.c in the Linux kernel before 2.6.34 does not properly manage a backlog of received packets, which allows remote attackers to cause a denial of service (memory consumption) by sending a large amount of network traffic, as demonstrated by netperf UDP tests.
- CVE-2010-4805: (linux kernel: Uncontrolled Resource Consumption)
  The socket implementation in net/core/sock.c in the Linux kernel before 2.6.35 does not properly manage a backlog of received packets, which allows remote attackers to cause a denial of service by sending a large amount of network traffic, related to the sk_add_backlog function and the sk_rmem_alloc socket field. NOTE: this vulnerability exists because of an incomplete fix for CVE-2010-4251.
- CVE-2011-0709: (linux kernel: NULL Pointer Dereference)
  The br_mdb_ip_get function in net/bridge/br_multicast.c in the Linux kernel before 2.6.35-rc5 allows remote attackers to cause a denial of service (NULL pointer dereference and system crash) via an IGMP packet, related to lack of a multicast table.
- CVE-2011-2525: (linux kernel: NULL Pointer Dereference)
  The qdisc_notify function in net/sched/sch_api.c in the Linux kernel before 2.6.35 does not prevent tc_fill_qdisc function calls referencing builtin (aka CQ_F_BUILTIN) Qdisc structures, which allows local users to cause a denial of service (NULL pointer dereference and OOPS) or possibly have unspecified other impact via a crafted call.
- CVE-2012-0207: (linux kernel: Divide By Zero)
  The igmp_heard_query function in net/ipv4/igmp.c in the Linux kernel before 3.2.1 allows remote attackers to cause a denial of service (divide-by-zero error and panic) via IGMP packets.
- CVE-2012-2136: (linux kernel: Improper Input Validation)
  The sock_alloc_send_pskb function in net/core/sock.c in the Linux kernel before 3.4.5 does not properly validate a certain length value, which allows local users to cause a denial of service (heap-based buffer overflow and system crash) or possibly gain privileges by leveraging access to a TUN/TAP device.
- CVE-2012-3552: (linux kernel: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition'))
  Race condition in the IP implementation in the Linux kernel before 3.0 might allow remote attackers to

cause a denial of service (slab corruption and system crash) by sending packets to an application that sets socket options during the handling of network traffic.

- CVE-2012-6638: (linux kernel: Resource Management Errors)
  The tcp_rcv_state_process function in net/ipv4/tcp_input.c in the Linux kernel before 3.2.24 allows remote attackers to cause a denial of service (kernel resource consumption) via a flood of SYN+FIN TCP packets, a different vulnerability than CVE-2012-2663.
- CVE-2012-6701: (linux kernel: Other)
  Integer overflow in fs/aio.c in the Linux kernel before 3.4.1 allows local users to cause a denial of service or possibly have unspecified other impact via a large AIO iovec.
- CVE-2012-6704: (linux kernel: Improper Restriction of Operations within the Bounds of a Memory Buffer)
  The sock_setsockopt function in net/core/sock.c in the Linux kernel before 3.5 mishandles negative values of sk_sndbuf and sk_rcvbuf, which allows local users to cause a denial of service (memory corruption and system crash) or possibly have unspecified other impact by leveraging the CAP_NET_ADMIN capability for a crafted setsockopt system call with the (1) SO_SNDBUF or (2) SO_RCVBUF option.
- CVE-2013-7470: (linux kernel: Uncontrolled Resource Consumption)
  cipso_v4_validate in include/net/cipso_ipv4.h in the Linux kernel before 3.11.7, when CONFIG_NETLABEL is disabled, allows attackers to cause a denial of service (infinite loop and crash), as demonstrated by icmpsic, a different vulnerability than CVE-2013-0310.
- CVE-2014-2523: (linux kernel: Improper Input Validation)
  net/netfilter/nf_conntrack_proto_dccp.c in the Linux kernel through 3.13.6 uses a DCCP header pointer incorrectly, which allows remote attackers to cause a denial of service (system crash) or possibly execute arbitrary code via a DCCP packet that triggers a call to the (1) dccp_new, (2) dccp_packet, or (3) dccp_error function.
- CVE-2015-1465: (linux kernel: DEPRECATED: Code)
  The IPv4 implementation in the Linux kernel before 3.18.8 does not properly consider the length of the Read-Copy Update (RCU) grace period for redirecting lookups in the absence of caching, which allows remote attackers to cause a denial of service (memory consumption or system crash) via a flood of packets.
- CVE-2015-5364: (linux kernel: Resource Management Errors)
  The (1) udp_recvmsg and (2) udpv6_recvmsg functions in the Linux kernel before 4.0.6 do not properly consider yielding a processor, which allows remote attackers to cause a denial of service (system hang) via incorrect checksums within a UDP packet flood.
- CVE-2016-10229: (linux kernel: Improperly Implemented Security Check for Standard)
  udp.c in the Linux kernel before 4.5 allows remote attackers to execute arbitrary code via UDP traffic that triggers an unsafe second checksum calculation during execution of a recv system call with the MSG_PEEK flag.
- CVE-2016-3134: (linux kernel: Improper Restriction of Operations within the Bounds of a Memory Buffer)
  The netfilter subsystem in the Linux kernel through 4.5.2 does not validate certain offset fields, which allows local users to gain privileges or cause a denial of service (heap memory corruption) via an IPT_SO_SET_REPLACE setsockopt call.
- CVE-2016-4997: (linux kernel: Permissions, Privileges, and Access Controls)
  The compat IPT_SO_SET_REPLACE and IP6T_SO_SET_REPLACE setsockopt implementations in the netfilter subsystem in the Linux kernel before 4.6.3 allow local users to gain privileges or cause a denial of service (memory corruption) by leveraging in-container root access to provide a crafted offset value that triggers an unintended decrement.

- CVE-2016-7039: (linux kernel: Resource Management Errors)
  The IP stack in the Linux kernel through 4.8.2 allows remote attackers to cause a denial of service (stack consumption and panic) or possibly have unspecified other impact by triggering use of the GRO path for large crafted packets, as demonstrated by packets that contain only VLAN headers, a related issue to CVE-2016-8666.
- CVE-2016-7117: (linux kernel: Data Processing Errors)
  Use-after-free vulnerability in the __sys_recvmmsg function in net/socket.c in the Linux kernel before 4.5.2 allows remote attackers to execute arbitrary code via vectors involving a recvmmsg system call that is mishandled during error processing.
- CVE-2016-8666: (linux kernel: Uncontrolled Resource Consumption)
  The IP stack in the Linux kernel before 4.6 allows remote attackers to cause a denial of service (stack consumption and panic) or possibly have unspecified other impact by triggering use of the GRO path for packets with tunnel stacking, as demonstrated by interleaved IPv4 headers and GRE headers, a related issue to CVE-2016-7039.
- CVE-2017-1000111: (linux kernel: Out-of-bounds Write)
  Linux kernel: heap out-of-bounds in AF_PACKET sockets. This new issue is analogous to previously disclosed CVE-2016-8655. In both cases, a socket option that changes socket state may race with safety checks in packet_set_ring. Previously with PACKET_VERSION. This time with PACKET_RESERVE. The solution is similar: lock the socket for the update. This issue may be exploitable, we did not investigate further. As this issue affects PF_PACKET sockets, it requires CAP_NET_RAW in the process namespace. But note that with user namespaces enabled, any process can create a namespace in which it has CAP_NET_RAW.
- CVE-2017-11176: (linux kernel: Use After Free)
  The mq_notify function in the Linux kernel through 4.11.9 does not set the sock pointer to NULL upon entry into the retry logic. During a user-space close of a Netlink socket, it allows attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact.
- CVE-2017-7618: (linux kernel: Loop with Unreachable Exit Condition ('Infinite Loop'))
  crypto/ahash.c in the Linux kernel through 4.10.9 allows attackers to cause a denial of service (API operation calling its own callback, and infinite recursion) by triggering EBUSY on a full queue.
- CVE-2017-8890: (linux kernel: Double Free)
  The inet_csk_clone_lock function in net/ipv4/inet_connection_sock.c in the Linux kernel through 4.10.15 allows attackers to cause a denial of service (double free) or possibly have unspecified other impact by leveraging use of the accept system call.
- CVE-2019-16746: (linux kernel: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow'))
  An issue was discovered in net/wireless/nl80211.c in the Linux kernel through 5.2.17. It does not check the length of variable elements in a beacon head, leading to a buffer overflow.
- CVE-2019-3896: (linux kernel: Multiple vulnerabilities including Double Free, Use After Free)
  A double-free can happen in idr_remove_all() in lib/idr.c in the Linux kernel 2.6 branch. An unprivileged local attacker can use this flaw for a privilege escalation or for a system crash and a denial of service (DoS).
- CVE-2010-3848: (linux kernel: Out-of-bounds Write)
  Stack-based buffer overflow in the econet_sendmsg function in net/econet/af_econet.c in the Linux kernel before 2.6.36.2, when an econet address is configured, allows local users to gain privileges by providing a large number of iovec structures.
- CVE-2012-0056: (linux kernel: Permissions, Privileges, and Access Controls)
  The mem_write function in the Linux kernel before 3.2.2, when ASLR is disabled, does not properly check permissions when writing to /proc/<pid>/mem, which allows local users to gain privileges by modifying

process memory, as demonstrated by Mempodipper.

- CVE-2010-2692: (custom t-shirt design script: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'))
  Cross-site scripting (XSS) vulnerability in 2daybiz Custom T-Shirt Design Script allows remote attackers to inject arbitrary web script or HTML via a review comment.
- CVE-2006-2937: (openssl: Resource Management Errors)
  OpenSSL 0.9.7 before 0.9.7l and 0.9.8 before 0.9.8d allows remote attackers to cause a denial of service (infinite loop and memory consumption) via malformed ASN.1 structures that trigger an improperly handled error condition.
- CVE-2006-2940: (openssl: Resource Management Errors)
  OpenSSL 0.9.7 before 0.9.7l, 0.9.8 before 0.9.8d, and earlier versions allows attackers to cause a denial of service (CPU consumption) via parasitic public keys with large (1) "public exponent" or (2) "public modulus" values in X.509 certificates that require extra time to process when using RSA signature verification.
- CVE-2006-3738: (openssl: Improper Restriction of Operations within the Bounds of a Memory Buffer)
  Buffer overflow in the SSL_get_shared_ciphers function in OpenSSL 0.9.7 before 0.9.7l, 0.9.8 before 0.9.8d, and earlier versions has unspecified impact and remote attack vectors involving a long list of ciphers.
- CVE-2009-3245: (openssl: Improper Input Validation)
  OpenSSL before 0.9.8m does not check for a NULL return value from bn_wexpand function calls in (1) crypto/bn/bn_div.c, (2) crypto/bn/bn_gf2m.c, (3) crypto/ec/ec2_smpl.c, and (4) engines/e_ubsec.c, which has unspecified impact and context-dependent attack vectors.
- CVE-2010-0742: (openssl: Cryptographic Issues)
  The Cryptographic Message Syntax (CMS) implementation in crypto/cms/cms_asn1.c in OpenSSL before 0.9.8o and 1.x before 1.0.0a does not properly handle structures that contain OriginatorInfo, which allows context-dependent attackers to modify invalid memory locations or conduct double-free attacks, and possibly execute arbitrary code, via unspecified vectors.
- CVE-2010-3864: (openssl: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition'))
  Multiple race conditions in ssl/t1_lib.c in OpenSSL 0.9.8f through 0.9.8o, 1.0.0, and 1.0.0a, when multi-threading and internal caching are enabled on a TLS server, might allow remote attackers to execute arbitrary code via client data that triggers a heap-based buffer overflow, related to (1) the TLS server name extension and (2) elliptic curve cryptography.
- CVE-2010-4252: (openssl: Improper Authentication)
  OpenSSL before 1.0.0c, when J-PAKE is enabled, does not properly validate the public parameters in the J-PAKE protocol, which allows remote attackers to bypass the need for knowledge of the shared secret, and successfully authenticate, by sending crafted values in each round of the protocol.
- CVE-2012-2110: (openssl: Improper Restriction of Operations within the Bounds of a Memory Buffer)
  The asn1_d2i_read_bio function in crypto/asn1/a_d2i_fp.c in OpenSSL before 0.9.8v, 1.0.0 before 1.0.0i, and 1.0.1 before 1.0.1a does not properly interpret integer data, which allows remote attackers to conduct buffer overflow attacks, and cause a denial of service (memory corruption) or possibly have unspecified other impact, via crafted DER data, as demonstrated by an X.509 certificate or an RSA public key.
- CVE-2014-3512: (openssl: Improper Restriction of Operations within the Bounds of a Memory Buffer)
  Multiple buffer overflows in crypto/srp/srp_lib.c in the SRP implementation in OpenSSL 1.0.1 before 1.0.1i allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via an invalid SRP (1) g, (2) A, or (3) B parameter.

- CVE-2014-3567: (openssl: Multiple vulnerabilities including Improper Input Validation, Resource Management Errors)
  Memory leak in the tls_decrypt_ticket function in t1_lib.c in OpenSSL before 0.9.8zc, 1.0.0 before 1.0.0o, and 1.0.1 before 1.0.1j allows remote attackers to cause a denial of service (memory consumption) via a crafted session ticket that triggers an integrity-check failure.
- CVE-2014-8176: (openssl: Improper Restriction of Operations within the Bounds of a Memory Buffer)
  The dtls1_clear_queues function in ssl/d1_lib.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h frees data structures without considering that application data can arrive between a ChangeCipherSpec message and a Finished message, which allows remote DTLS peers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact via unexpected application data.
- CVE-2015-0292: (openssl: Improper Restriction of Operations within the Bounds of a Memory Buffer)
  Integer underflow in the EVP_DecodeUpdate function in crypto/evp/encode.c in the base64-decoding implementation in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via crafted base64 data that triggers a buffer overflow.
- CVE-2016-2108: (openssl: Improper Restriction of Operations within the Bounds of a Memory Buffer)
  The ASN.1 implementation in OpenSSL before 1.0.1o and 1.0.2 before 1.0.2c allows remote attackers to execute arbitrary code or cause a denial of service (buffer underflow and memory corruption) via an ANY field in crafted serialized data, aka the "negative zero" issue.
- CVE-2016-2109: (openssl: Resource Management Errors)
  The asn1_d2i_read_bio function in crypto/asn1/a_d2i_fp.c in the ASN.1 BIO implementation in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to cause a denial of service (memory consumption) via a short invalid encoding.