Severity

High

Analysis Summary

CVE-2022-20695 CVSS: 10

A vulnerability in the authentication functionality of Cisco Wireless LAN Controller (WLC) Software could allow an unauthenticated, remote attacker to bypass authentication controls and log in to the device through the management interface

This vulnerability is due to the improper implementation of the password validation algorithm. An attacker could exploit this vulnerability by logging in to an affected device with crafted credentials. A successful exploit could allow the attacker to bypass authentication and log in to the device as an administrator. The attacker could obtain privileges that are the same level as an administrative user but it depends on the crafted credentials.

CVE-2022-20739 CVSS: 7.3

A vulnerability in the CLI of Cisco SD-WAN vManage Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system as the root user. The attacker must be authenticated on the affected system as a low-privileged user to exploit this vulnerability.

This vulnerability exists because a file leveraged by a root user is executed when a low-privileged user runs specific commands on an affected system. An attacker could exploit this vulnerability by injecting arbitrary commands to a specific file as a lower-privileged user and then waiting until an admin user executes specific commands. The commands would then be executed on the device by the root user. A successful exploit could allow the attacker to escalate their privileges on the affected system from a low-privileged user to the root user.

CVE-2022-20716 CVSS: 7.8

A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to gain escalated privileges.

This vulnerability is due to improper access control on files within the affected system. A local attacker could exploit this vulnerability by modifying certain files on the vulnerable device. If successful, the attacker could gain escalated privileges and take actions on the system with the privileges of the root user.

CVE-2022-20692 CVSS: 7.7

A vulnerability in the NETCONF over SSH feature of Cisco IOS XE Software could allow a low-privileged, authenticated, remote attacker to cause a denial of service condition (DoS) on an affected device.

This vulnerability is due to insufficient resource management. An attacker could exploit this vulnerability by initiating a large number of NETCONF over SSH connections. A successful exploit could allow the attacker to exhaust resources, causing the device to reload and resulting in a DoS condition on an affected device.

CVE-2022-20714 CVSS: 8.6

A vulnerability in the data plane microcode of Lightspeed-Plus line cards for Cisco ASR 9000 Series Aggregation Services Routers could allow an unauthenticated, remote attacker to cause the line card to reset.

This vulnerability is due to the incorrect handling of malformed packets that are received on the Lightspeed-Plus line cards. An attacker could exploit this vulnerability by sending a crafted IPv4 or IPv6 packet through an affected device. A successful exploit could allow the attacker to cause the Lightspeed-Plus line card to reset, resulting in a denial of service (DoS) condition for any traffic that traverses that line card.

CVE-2022-20697 CVSS: 8.6

A vulnerability in the web services interface of Cisco IOS Software and Cisco IOS XE Software could allow an authenticated, remote attacker to cause a denial of service (DoS) condition.

This vulnerability is due to improper resource management in the HTTP server code. An attacker could exploit this vulnerability by sending a large number of HTTP requests to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition.

CVE-2022-20681 CVSS: 7.8

A vulnerability in the CLI of Cisco IOS XE Software for Cisco Catalyst 9000 Family Switches and Cisco Catalyst 9000 Family Wireless Controllers could allow an authenticated, local attacker to elevate privileges to level 15 on an affected device.

This vulnerability is due to insufficient validation of user privileges after the user executes certain CLI commands. An attacker could exploit this vulnerability by logging in to an affected device as a low-privileged user and then executing certain CLI commands. A successful exploit could allow the attacker to execute arbitrary commands with level 15 privileges on the affected device.

CVE-2022-20761 CVSS: 7.4

A vulnerability in the integrated wireless access point (AP) packet processing of the Cisco 1000 Series Connected Grid Router (CGR1K) could allow an unauthenticated, adjacent attacker to cause a denial of service condition on an affected device.

This vulnerability is due to insufficient input validation of received traffic. An attacker could exploit this vulnerability by sending crafted traffic to an affected device. A successful exploit could allow the attacker to cause the integrated AP to stop processing traffic, resulting in a DoS condition. It may be necessary to manually reload the CGR1K to restore AP operation.

CVE-2022-20661; CVE-2022-20731 CVSS: 6.8

Multiple vulnerabilities that affect Cisco Catalyst Digital Building Series Switches and Cisco Catalyst Micro Switches could allow an attacker to execute persistent code at boot time or to permanently prevent the device from booting, resulting in a permanent denial of service (DoS) condition.

CVE-2022-20684 CVSS: 7.4

A vulnerability in Simple Network Management Protocol (SNMP) trap generation for wireless clients of Cisco IOS XE Wireless Controller Software for the Catalyst 9000 Family could allow an unauthenticated, adjacent attacker to cause an affected device to unexpectedly reload, resulting in a denial of service (DoS) condition on the device.

This vulnerability is due to a lack of input validation of the information used to generate an SNMP trap related to a wireless client connection event. An attacker could exploit this vulnerability by sending an 802.1x packet with crafted parameters during the wireless authentication setup phase of a connection. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition.

CVE-2022-20683 CVSS: 8.6

A vulnerability in the Application Visibility and Control (AVC-FNF) feature of Cisco IOS XE Software for Cisco Catalyst 9800 Series Wireless Controllers could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device.

This vulnerability is due to insufficient packet verification for traffic inspected by the AVC feature. An attacker could exploit this vulnerability by sending crafted packets from the wired network to a wireless client, resulting in the crafted packets being processed by the wireless controller. A successful exploit could allow the attacker to cause a crash and reload of the affected device, resulting in a DoS condition.

CVE-2022-20682 CVSS: 8.6

A vulnerability in the Control and Provisioning of Wireless Access Points (CAPWAP) protocol processing of Cisco IOS XE Wireless Controller Software for the Catalyst 9000 Family could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device.

This vulnerability is due to inadequate input validation of incoming CAPWAP packets encapsulating multicast DNS (mDNS) queries. An attacker could exploit this vulnerability by connecting to a wireless network and sending a crafted mDNS query, which would flow through and be processed by the wireless controller. A successful exploit could allow the attacker to cause the affected device to crash and reload, resulting in a DoS condition.

CVE-2022-20678 CVSS: 8.6

A vulnerability in the AppNav-XE feature of Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause an affected device to reload, resulting in a denial of service (DoS) condition.

This vulnerability is due to the incorrect handling of certain TCP segments. An attacker could exploit this vulnerability by sending a stream of crafted TCP traffic at a high rate through an interface of an affected device. That interface would need to have AppNav interception enabled. A successful exploit could allow the attacker to cause the device to reload.

CVE-2022-20622 CVSS: 8.6

A vulnerability in IP ingress packet processing of the Cisco Embedded Wireless Controller with Catalyst Access Points Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, causing a denial of service (DoS) condition. The device may experience a performance degradation in traffic processing or high CPU usage prior to the unexpected reload.

This vulnerability is due to improper rate limiting of IP packets to the management interface. An attacker could exploit this vulnerability by sending a steady stream of IP traffic at a high rate to the management interface of the affected device. A successful exploit could allow the attacker to cause the device to reload.

CVE-2022-20693 CVSS: 4.7

A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to perform an injection attack against an affected device.

This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI API. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges.

CVE-2022-20735 CVSS: 6.5

A vulnerability in the web-based management interface of Cisco SD-WAN vManage Software could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack on an affected system.

This vulnerability is due to insufficient CSRF protections for the web-based management interface on an affected system. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link. A successful exploit could allow the attacker to perform arbitrary actions with the privilege level of the affected user. These actions could include modifying the system configuration and deleting accounts.

CVE-2022-20717 CVSS: 5.5

A vulnerability in the NETCONF process of Cisco SD-WAN vEdge Routers could allow an authenticated, local attacker to cause an affected device to run out of memory, resulting in a denial of service (DoS) condition.

This vulnerability is due to insufficient memory management when an affected device receives large amounts of traffic. An attacker could exploit this vulnerability by sending malicious traffic to an affected device. A successful exploit could allow the attacker to cause the device to crash, resulting in a DoS condition.

CVE-2022-20679 CVSS: 6.8

A vulnerability in the IPSec decryption routine of Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause an affected device to reload, resulting in a denial of service (DoS) condition.

This vulnerability is due to buffer exhaustion that occurs while traffic on a configured IPsec tunnel is being processed. An attacker could exploit this vulnerability by sending traffic to an affected device that has a maximum transmission unit (MTU) of 1800 bytes or greater. A successful exploit could allow the attacker to cause the device to reload.

CVE-2022-20677; CVE-2022-20718; CVE-2022-20719; CVE-2022-20720; CVE-2022-20721; CVE-2022-20722; CVE-2022-20723; CVE-2022-20724; CVE-2022-20725; CVE-2022-20726; CVE-2022-20727 CVSS: 5.5

Multiple vulnerabilities in the Cisco IOx application hosting environment on multiple Cisco platforms could allow an attacker to inject arbitrary commands into the underlying host operating system, execute arbitrary code on the underlying host operating system, install applications without being authenticated, or conduct a cross-site scripting (XSS) attack against a user of the affected software.

CVE-2022-20694 CVSS: 6.8

A vulnerability in the implementation of the Resource Public Key Infrastructure (RPKI) feature of Cisco IOS XE 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 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-2022-20676 CVSS: 5.1

A vulnerability in the Tool Command Language (Tcl) interpreter of Cisco IOS XE Software could allow an authenticated, local attacker to escalate from privilege level 15 to root-level privileges.

This vulnerability is due to insufficient input validation of data that is passed into the Tcl interpreter. An attacker could exploit this vulnerability by loading malicious Tcl code on an affected device. A successful exploit could allow the attacker to execute arbitrary commands as root. By default, Tcl shell access requires privilege level 15.

CVE-2022-20758 CVSS: 6.8

A vulnerability in the implementation of the Border Gateway Protocol (BGP) Ethernet VPN (EVPN) functionality in Cisco IOS XR Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition.

This vulnerability is due to the incorrect processing of a BGP update message that contains specific EVPN attributes. An attacker could exploit this vulnerability by sending a BGP update message that contains specific EVPN attributes. To exploit this vulnerability, an attacker must control a BGP speaker that has an established trusted peer connection to an affected device that is configured with the address family L2VPN EVPN to receive and process the update message. This vulnerability cannot be exploited by any data that is initiated by clients on the Layer 2 network or by peers that are not configured to accept the L2VPN EVPN address family. A successful exploit could allow the attacker to cause the BGP process to restart unexpectedly, resulting in a DoS condition.

Impact

- Denial of Service
- Information Disclosure
- Data Exfiltration
- Privilege Escalation
- Improper Access
- Authentication Bypass

Affected Vendors

Cisco

Affected Products

- 3504 Wireless Controller
- 5520 Wireless Controller
- 8540 Wireless Controller
- Virtual Wireless Controller (vWLC)
- Cisco SD-WAN vBond Orchestrator Software
- SD-WAN vEdge Cloud Routers
- SD-WAN vSmart Controller Software
- Cisco IOS-XR 64-bit Software

- Catalyst 9800 Embedded Wireless Controllers for Catalyst 9300
- 9400
- and 9500 Series Switches
- Catalyst 9800 Series Wireless Controllers
- Catalyst 9800-CL Wireless Controllers for Cloud
- Embedded Wireless Controllers on Catalyst Access Points

Remediation

Refer to the following vendor website for patches, updates, and workarounds.

Cisco