CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2021-053

Critical Vulnerabilities in Cisco Software

September 24, 2021 — v1.0

TLP:WHITE

History:

- *24/09/2021 — v1.0 – Initial publication*

Summary

On Wednesday, September 22, 2021, Cisco Product Security Incident Response Team (PSIRT) has released 31 security advisories (**3 Critical**, 13 High, 15 Medium) to address multiple vulnerabilities in Cisco IOS XE software or products running with a specific configuration [1]. At this time, the Cisco (PSIRT) is not aware of any public announcements or malicious use of the critical vulnerabilities CVE-2021-34770, CVE-2021-34727 and CVE-2021-1619 [2,3,4].

Technical Details

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 [2].

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 [2].

CVE-2021-34727 Cisco IOS XE SD-WAN Software Buffer Overflow vulnerability

A vulnerability in the vDaemon process in Cisco IOS XE SD-WAN Software could allow an unauthenticated, remote attacker to cause a buffer overflow on an affected device [3].

This vulnerability is due to insufficient bounds checking when an affected device processes traffic. An attacker could exploit this vulnerability by sending crafted traffic to the device. A successful exploit could allow the attacker to cause a buffer overflow and possibly execute arbitrary commands with root-level privileges, or cause the device to reload, which could result in a denial of service condition [3].

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 [4]:

- 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 [4].

Affected Products

CVE-2021-34770

This vulnerability affects the following Cisco products if they are running a vulnerable release of Cisco IOS XE Software for Cisco Catalyst 9000 Family Wireless Controllers [2]:

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

CVE-2021-34727

This vulnerability affects the following Cisco products if they are running a vulnerable release of Cisco IOS XE SD-WAN Software and have the SD-WAN feature enabled [3]:

- 1000 Series Integrated Services Routers (ISRs)
- 4000 Series ISRs
- ASR 1000 Series Aggregation Services Routers
- Cloud Services Router 1000V Series

CVE-2021-1619

This vulnerability affects Cisco IOS XE Software if it is running in autonomous or controller mode and Cisco IOS XE SD-WAN Software. For either to be affected, all of the following must be configured [4]:

- `AAA`,
- `NETCONF`, `RESTCONF`, or both,
- enable password without enable secret.

Recommendations

Cisco has released software updates that address these vulnerabilities.

CERT-EU recommends updating the vulnerable application as soon as possible.

Workarounds and Mitigations

There is a workaround that addresses **CVE-2021-1619** vulnerability:

- Remove the *enable password* and configure the *enable secret* [4,5].
- To limit the attack surface of this vulnerability, ensure that access control lists (ACLs) are in place for `NETCONF` and `RESTCONF` to prevent attempted access from untrusted subnets [4,6].

There are no workarounds for **CVE-2021-34770** and **CVE-2021-34727** vulnerabilities [2,3].

References

[1] https://tools.cisco.com/security/center/publicationListing.x

[2] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ewlc-capwap-rce-LYgj8Kf

[3] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxesdwan-rbuffover-vE2OB6tp

[4] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aaa-Yx47ZT8Q

[5] https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html#anc14

[6] https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/prog/configuration/1611/b_1611_programmability_cg/service_level_ACLs_NETCONF_RESTCONF.html