Security Advisory 2021-003

Critical Vulnerabilities in Cisco SD WAN

January 21, 2021 — v1.0

TLP:WHITE

History:

- *21/01/2021 — v1.0 – Initial publication*

Summary

Cisco has published an advisory about several vulnerabilities affecting Cisco SD-WAN software [1-4]. These vulnerabilities could lead to **remote code execution**, **denial of service**, or **authtication bypass**. While Cisco is not aware of any malicious exploit in the wild, it is highly recommended to patch the affected products.

Technical Details

This advisory only describes the most critical vulnerabilities disclosed by Cisco.

CVE-2021-1300

The first vulnerability, identified by **CVE-2021-1300**, is due to incorrect handling of IP traffic by the SD-WAN software. By sending crafted packets to a vulnerable device, an **unauthenticated, remote** attacker could cause a **buffer overflow** on the underlying software. Successfully exploiting this vulnerability could lead the attacker to execute arbitrary code on the operating system with **root** privileges. The CVSS score of this vulnerability is **9.8**

CVE-2021-1302

The second vulnerability, identified by **CVE-2021-1302**, is due to insufficient authorization checks. An attacker could exploit this vulnerability by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the **unauthenticated** attacker to bypass authorization and connect to other vManage tenants that they are not authorized to connect to. The CVSS score of this vulnerability is **8.8**

CVE-2021-1299

The third vulnerability, identified by **CVE-2021-1299**, is due to improper input validation of user-supplied input to the device template configuration. An **authenticated** attacker could exploit this vulnerability by submitting crafted input to the device template configuration. A successful exploit could allow the attacker to gain root-level access to the affected system. The CVSS score of this vulnerability is **9.9**

CVE-2021-1241

The forth vulnerability, identified by **CVE-2021-1241**, is due to insufficient handling of malformed packets. An **unauthenticated** attacker could exploit this vulnerability by sending crafted packets through an affected device. A successful exploit could allow the attacker to cause the device to reboot, resulting in a DoS condition on the affected system. The CVSS score of this vulnerability is **8.6**

CVE-2021-1273

The fifth vulnerability, identified by **CVE-2021-1273**, is due to the bounds checking in the forwarding plane of the IPSec tunnel management functionality. An **unauthenticated, remote** attacker could exploit this vulnerability by sending crafted IPv4 or IPv6 packets to a specific device. A successful exploit could allow the attacker to cause a DoS condition on the affected system. The CVSS score of this vulnerability is **8.6**

CVE-2021-1274

The sixth vulnerability, identified by **CVE-2021-1274**, is due to the presence of a null dereference in vDaemon. An **unauthenticated, remote** attacker could exploit this vulnerability by sending crafted traffic to a specific device. A successful exploit could allow the attacker to cause a DoS condition on the affected system. The CVSS score of this vulnerability is **8.6**

Affected products

The following products could be affected by the vulnerabilities:

- IOS XE SD-WAN Software
- SD-WAN vBond Orchestrator Software
- SD-WAN vEdge Cloud Routers
- SD-WAN vEdge Routers
- SD-WAN vManage Software
- SD-WAN vSmart Controller Software

The following software releases are affected by the vulnerabilities:

- SD-WAN Software
  - release versions prior to 20.3
  - release version 20.3 prior to 20.3.2
  - release version 20.4 prior to 20.4.1
- IOS XE SD-WAN Software
  - release versions prior to 16.12
  - release version 16.12 prior to 16.12.4
- IOS XE Software
  - release version 17.2 prior to 17.2.2
  - release version 17.3 prior to 17.3.1
  - release version 17.4 prior to 17.4.1

Recommendations

It is recommended to apply the patches from Cisco for all affected software and products.

References

[1] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-bufovulns-B5NrSHbj

[2] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-abyp-TnGFHrS

[3] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn

[4] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dosmulti-48jJuEUP

[4] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dosmulti-48jJuEUP