Security Advisory 2020-039

Critical Vulnerabilities in Cisco Products

July 30, 2020 — v1.0

TLP:WHITE

History:

- *30/07/2020 — v1.0 – Initial publication*

Summary

On 29th of July, Cisco released several security updates to address security vulnerabilities including three critical ones: an authentication bypass (CVE-2020-3382), a buffer overflow (CVE-2020-3375), and an authorization bypass (CVE-2020-3374). Additionally, Cisco issued an advisory update v1.7 for a series of critical vulnerabilities (first published on 17th of June) related to Treck IP stack (from CVE-2020-11896 to CVE-2020-11914) [1, 6].

Moreover, the company also issued security updates to fix another eight high and medium severity vulnerabilities found to affect several other Cisco Data Center Network Manager (DCNM) Software versions (CVE-2020-3377, CVE-2020-3384, CVE-2020-3383, CVE-2020-3386, CVE-2020-3376, CVE-2020-3460, CVE-2020-3462, CVE-2020-3461) [1, 2].

Technical Details

CVE-2020-3375 (CVSS Score: Base 9.8)

A vulnerability in Cisco SD-WAN Solution Software could allow an unauthenticated, remote attacker to cause a buffer overflow on an affected device. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted traffic to an affected device. A successful exploit could allow the attacker to gain access to information that they are not authorized to access, make changes to the system that they are not authorized to make, and execute commands on an affected system with privileges of the root user [3].

CVE-2020-3374 (CVSS Score: Base 9.9)

A vulnerability in the web-based management interface of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to bypass authorization, enabling them to access sensitive information, modify the system configuration, or impact the availability of the affected system. The vulnerability is due to insufficient authorization checking on the affected system. 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

attacker to gain privileges beyond what would normally be authorized for their configured user authorization level. The attacker may be able to access sensitive information, modify the system configuration, or impact the availability of the affected system [4].

CVE-2020-3382 (CVSS Score: Base 9.8)

A vulnerability in the REST API of Cisco Data Center Network Manager (DCNM) could allow an unauthenticated, remote attacker to bypass authentication and execute arbitrary actions with administrative privileges on an affected device. The vulnerability exists because different installations share a static encryption key. An attacker could exploit this vulnerability by using the static key to craft a valid session token. A successful exploit could allow the attacker to perform arbitrary actions through the REST API with administrative privileges [5].

CVE-2020-11896, CVE-2020-11897, CVE-2020-11898, CVE-2020-11899, CVE-2020-11900, CVE-2020-11901, CVE-2020-11902, CVE-2020-11903, CVE-2020-11904, CVE-2020-11905, CVE-2020-11906, CVE-2020-11907, CVE-2020-11908, CVE-2020-11909, CVE-2020-11910, CVE-2020-11911, CVE-2020-11912, CVE-2020-11913, CVE-2020-11914 (Cisco Bug IDs: CSCvu68945)

Vulnerabilities on the Treck IP stack implementation are collectively known as Ripple20. Exploitation of these vulnerabilities could result in remote code execution, denial of service (DoS), or information disclosure, depending on the specific vulnerability [6].

The Cisco Product Security Incident Response Team (PSIRT) is not aware of any malicious use of these vulnerabilities [2, 6].

Products Affected

These vulnerabilities affect several products:

- IOS XE SD-WAN Software [3, 4];
- SD-WAN vBond Orchestrator Software [3, 4];
- SD-WAN vEdge Cloud Routers [3];
- SD-WAN vEdge Routers [3, 4];
- SD-WAN vManage Software [3];
- SD-WAN vSmart Controller Software [3, 4];
- DCNM software releases 11.0(1), 11.1(1), 11.2(1), and 11.3(1) [5];
- ASR 5000 [6];
- ASR 5500 [6];
- Virtual Packet Core [6];
- StarOS Software [6].

Recommendations

Cisco has released free software updates that address critical (CVE-2020-3375, CVE-2020-3374, CVE-2020-3382), as well as high and medium vulnerabilities [1].

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

In addition, for information about fixed Treck IP stack vulnerabilities (from CVE-2020-11896 to CVE-2020-11914), Cisco customers are advised to regularly consult the advisories for Cisco products to determine exposure and a complete upgrade solution [6].

Moreover, a set of network-based mitigation has been documented and is available in [7].

References

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

[2] https://www.bleepingcomputer.com/news/security/cisco-fixes-severe-flaws-in-data-center-management-solution/

[3] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdbufof-h5f5VSeL

[4] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-uabvman-SYGzt8Bv

[5] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dcnm-bypass-dyEejUMs

[6] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-treck-ip-stack-JyBQ5GyC

[7] https://github.com/CERTCC/PoC-Exploits/blob/master/vu-257161/recommendations.md