CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2021-012

Critical Vulnerabilities in Cisco Products

February 25, 2021 — v1.0

TLP:WHITE

Summary

On 24th of February 2021, Cisco released several security updates to address security vulnerabilities including three critical ones: an authentication bypass (CVE-2021-1388) [1], an unauthenticated arbitrary file actions (CVE-2021-1361) [2], and an unauthorised access (CVE-2021-1393) [3].

Technical Details

CVE-2021-1388 (CVSS Score: Base 10)

A vulnerability in an API endpoint of Cisco ACI Multi-Site Orchestrator (MSO) installed on the Application Services Engine could allow an unauthenticated, remote attacker to bypass authentication on an affected device.

The vulnerability is due to improper token validation on a specific API endpoint. An attacker could exploit this vulnerability by sending a crafted request to the affected API. A successful exploit could allow the attacker to receive a token with administrator-level privileges that could be used to authenticate to the API on affected MSO and managed Cisco Application Policy Infrastructure Controller (APIC) devices.

CVE-2021-1361 (CVSS Score: Base 9.8)

A vulnerability in the implementation of an internal file management service for Cisco Nexus 3000 Series Switches and Cisco Nexus 9000 Series Switches in standalone NX-OS mode that are running Cisco NX-OS Software could allow an unauthenticated, remote attacker to create, delete, or overwrite arbitrary files with root privileges on the device.

This vulnerability exists because TCP port 9075 is incorrectly configured to listen and respond to external connection requests. An attacker could exploit this vulnerability by sending crafted TCP packets to an IP address that is configured on a local interface on TCP port 9075. A successful exploit could allow the attacker to create, delete, or overwrite arbitrary files, including sensitive files that are related to the device configuration. For example, the attacker could add a user account without the device administrator knowing.

CVE-2021-1393 (CVSS Score: Base 9.8)

Multiple vulnerabilities in Cisco Application Services Engine could allow an unauthenticated, remote attacker to gain privileged access to host-level operations or to learn device-specific information, create diagnostic files, and make limited configuration changes.

The vulnerability is due to insufficient access controls for a service running in the Data Network. An attacker could exploit this vulnerability by sending crafted TCP requests to a specific service. A successful exploit could allow the attacker to have privileged access to run containers or invoke host-level operations.

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

Products Affected

These vulnerabilities affect several products as follows:

CVE-2021-1388

- Cisco ACI Multi-Site Orchestrator (MSO) 3.0 (only when deployed on a Cisco Application Services Engine)

CVE-2021-1361

The following Cisco Products if they are running Cisco NX-OS Software Release 9.3(5) or Release 9.3(6):

- Nexus 3000 Series Switches
- Nexus 9000 Series Switches in standalone NX-OS mode

CVE-2021-1393

- Cisco Application Services Engine Software releases 1.1(3d) and earlier

Recommendations

Cisco has released software updates that address these critical vulnerabilities [1, 2, 3].

There are no workarounds that address CVE-2021-1388 and CVE-2021-1393 vulnerabilities. The CVE-2021-1361 has a workaround by using the infrastructure access control lists (iACLs) to allow only strictly required management and control plane traffic that is destined to the affected device [2].

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

References

[1] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-mso-authbyp-bb5GmBQv

[2] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-3000-9000-fileaction-QtLzDRy2

[3] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-case-mvuln-dYrDPC6w