CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2021-034

Vulnerabilities in Cisco Products

July 8, 2021 — v1.0

TLP:WHITE

History:

- *08/07/2021 — v1.0 – Initial publication*

Summary

On July 7, Cisco released security updates to address several security vulnerabilities [1]. This list includes vulnerabilities rated High affecting Cisco Business Process Automation (BPA) with a CVSS score of 8.8 out of 10 [2] and a vulnerability rated Medium affecting Cisco Adaptive Security Device Manager (ASDM) with a CVSS score of 7.5 out of 10 [3].

Vulnerabilities in Cisco Business Process Automation (BPA) could allow an authenticated, remote attacker to elevate privileges to Administrator. The vulnerability affecting Cisco Adaptive Security Device Manager (ASDM) could allow an unauthenticated, remote attacker to execute arbitrary code on a user's operating system.

Technical details

High vulnerabilities

CVE-2021-1574 and CVE-2021-1576

These vulnerabilities are due to improper authorisation enforcement for specific features and for access to log files that contain confidential information. An attacker could exploit these vulnerabilities either by submitting crafted HTTP messages to an affected system and performing unauthorised actions with the privileges of an administrator, or by retrieving sensitive data from the logs and using it to impersonate a legitimate privileged user. A successful exploit could allow the attacker to elevate privileges to Administrator [2].

Medium vulnerability

CVE-2021-1585

This vulnerability is due to a lack of proper signature verification for specific code exchanged between the ASDM and the Launcher. An attacker could exploit this vulnerability by leveraging a man-in-the-middle position on the network to intercept the traffic between the Launcher and the ASDM and then inject arbitrary code. A successful exploit could allow the attacker to execute arbitrary code on the user's operating system with the level of privileges assigned to the ASDM Launcher. A successful exploit may require the attacker to perform a social engineering attack to persuade the user to initiate communication from the Launcher to the ASDM [3].

Products affected

- CVE-2021-1574 and CVE-2021-1576 vulnerabilities affect Cisco BPA releases earlier than Release 3.1.
- CVE-2021-1585 vulnerability affects Cisco ASDM releases 9.16.1 and earlier.

Recommendations

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

There is no workaround that address these vulnerabilities.

CERT-EU recommends updating vulnerable applications as soon as possible.

References

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

[2] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-bpa-priv-esc-dgubwbH4

[3] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asdm-rce-gqjShXW