Security Advisory 2021-039

Cisco Intersight Virtual Appliance Forwarding Vulnerabilities

July 22, 2021 — v1.0

TLP:WHITE

History:

- *22/07/2021 — v1.0 – Initial publication*

Summary

Multiple vulnerabilities in Cisco Intersight Virtual Appliance could allow an unauthenticated, adjacent attacker to access sensitive internal services from an external interface [1].

Technical Details

These vulnerabilities (CVE-2021-1600, CVE-2021-1601) are due to insufficient restrictions for IPv4 or IPv6 packets that are received on the external management interface. An attacker could exploit these vulnerabilities by sending specific traffic to this interface on an affected device. A successful exploit could allow the attacker to access sensitive internal services and make configuration changes on the affected device [1].

Affected Products

The vulnerability with the Cisco Bug ID CSCvx84462 affects Cisco Intersight Virtual Appliance releases earlier than the first fixed release for IPv4 traffic.

The vulnerability with the Cisco Bug ID CSCvy29625 affects Cisco Intersight Virtual Appliance releases 1.0.9-184 to the first fixed release for IPv6 traffic.

These vulnerabilities do not affect customers who use Cisco Intersight Services for Cloud.

Recommendations

Cisco fixed these vulnerabilities for both IPv4 and IPv6 in Cisco Intersight Virtual Appliance releases 1.0.9-292 and later.

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

Workaround

There are no workarounds reported to address these vulnerabilities.

References

[1] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucsi2-iptaclbp-L8Dzs8m8