IP FABRIC

COMMON VULNERABILITIES AND EXPOSURES (CVE)

Report Introduction

The CVE Vulnerability report provides a comprehensive analysis of potential security vulnerabilities in network devices based on their operating system versions. The data is collected using IP Fabric's SDK and enriched with vulnerability information from the National Vulnerability Database (NVD).

This report includes detailed information about each device's operating system, known vulnerabilities, and their severity levels. It can be used to identify potential security risks and prioritize system updates or patches.

The analysis covers vendor-specific vulnerabilities and provides actionable insights for maintaining network security.

Snapshot Data Summary

IP Fabric URL	https://demo2.eu.ipfabric.io/api/v6.10/
IP Fabric Version	6.10.4+0
Snapshot Name	Day 4
Snapshot ID	224758b4-b66e-40e1-8584-d70d2e3ecf78
Network sites/groups	6
Network devices	49

1 Device Overview

Summary of devices and their vulnerability status

Hostname	Vendor	Family	Version	CVE Count
s3xdsw01	arista	eos	4.27.0F	10
s3xasw02	arista	eos	4.27.0F	10
s1xsw02	arista	eos	4.27.0F	10
s3xdsw03	arista	eos	4.27.0F	10
s1xsw06	arista	eos	4.27.0F	10
s3xdsw04	arista	eos	4.27.0F	10
s1xsw05	arista	eos	4.27.0F	10
s1xsw01	arista	eos	4.27.0F	10
s2xsw01	arista	eos	4.27.0F	10
s3xasw01	arista	eos	4.27.0F	10
s3xdsw02	arista	eos	4.27.0F	10
s1xsw04	arista	eos	4.27.0F	10
s1xsw03	arista	eos	4.27.0F	10
s3xasw03	arista	eos	4.27.0F	10
s3xasw04	arista	eos	4.27.0F	10

2 Summary Vulnerability Analysis

Security Risk Overview

Total CVEs

150

Critical/High CVEs

90

Avg CVSS Score

7.05

Vulnerability Severity Distribution

Severity	Count	Percentage
CRITICAL	0	0.0%
HIGH	90	60.0%
MEDIUM	60	40.0%
LOW	0	0.0%

3 Detailed Vulnerability Analysis

ARISTA EOS (4.27.0F) Details

Affected Hostnames:

[s3xasw04, s3xdsw04, s1xsw06, s1xsw04, s3xasw03, s3xdsw01, s1xsw03, s3xdsw02, s1xsw01, s3xasw01, s3xasw02, s1xsw05, s2xsw01, s1xsw02, s3xdsw03]

CVE List:

[CVE-2021-28504, CVE-2021-28505, CVE-2021-28508, CVE-2021-28509, CVE-2021-28511, CVE-2021-28510, CVE-2023-24511, CVE-2023-24509, CVE-2023-24512, CVE-2023-24510]

CVE Details:

CVE ID: **CVE-2021-28504**
Severity: metric_v3 **HIGH**
Impact Score: metric_v3 **3.6**
URL: https://www.arista.com/en/support/advisories-notices/security-advisories/15267-security-advisory-0073
Description

> On Arista Strata family products which have “TCAM profile” feature enabled when Port IPv4 access-list has a rule which matches on “vxlan” as protocol then that rule and subsequent rules (rules declared after it in ACL) do not match on IP protocol field as expected.

CVE ID: **CVE-2021-28505**
Severity: metric_v3 **HIGH**
Impact Score: metric_v3 **3.6**
URL: https://www.arista.com/en/support/advisories-notices/security-advisories/15267-security-advisory-0073
Description

> On affected Arista EOS platforms, if a VXLAN match rule exists in an IPv4 access-list that is applied to the ingress of an L2 or an L3 port/SVI, the VXLAN rule and subsequent ACL rules in that access list will ignore the specified IP protocol.

CVE ID: **CVE-2021-28508**
Severity: metric_v3 **MEDIUM**
Impact Score: metric_v3 **5.2**
URL: https://www.arista.com/en/support/advisories-notices/security-advisories/15484-security-advisory-0077
Description

> This advisory documents the impact of an internally found vulnerability in Arista EOS state streaming telemetry agent TerminAttr and OpenConfig transport protocols. The impact of this vulnerability is that, in certain conditions, TerminAttr might leak IPsec sensitive data in clear text in CVP to other authorized users, which could cause IPsec traffic to be decrypted or modified by other authorized users on the device.

CVE ID: **CVE-2021-28509**
Severity: metric_v3 **MEDIUM**
Impact Score: metric_v3 **5.2**
URL: https://www.arista.com/en/support/advisories-notices/security-advisories/15484-security-advisory-0077
Description

> This advisory documents the impact of an internally found vulnerability in Arista EOS state streaming telemetry agent TerminAttr and OpenConfig transport protocols. The impact of this vulnerability is that, in certain conditions, TerminAttr might leak MACsec sensitive data in clear text in CVP to other authorized users, which could cause MACsec traffic to be decrypted or modified by other authorized users on the device.

CVE ID: **CVE-2021-28511**
Severity: metric_v3 **MEDIUM**
Impact Score: metric_v3 **2.5**
URL: https://www.arista.com/en/support/advisories-notices/security-advisory/15862-security-advisory-0078
Description

> This advisory documents the impact of an internally found vulnerability in Arista EOS for security ACL bypass. The impact of this vulnerability is that the security ACL drop rule might be bypassed if a NAT ACL rule filter with permit action matches the packet flow. This could allow a host with an IP address in a range that matches the range allowed by a NAT ACL and a range denied by a Security ACL to be forwarded incorrectly as it should have been denied by the Security ACL. This can enable an ACL bypass.

CVE ID: **CVE-2021-28510**
Severity: metric_v3 **HIGH**
Impact Score: metric_v3 **3.6**
URL: https://www.arista.com/en/support/advisories-notices/security-advisory/15439-security-advisory-0076
Description

> For certain systems running EOS, a Precision Time Protocol (PTP) packet of a management/signaling message with an invalid Type-Length-Value (TLV) causes the PTP agent to restart. Repeated restarts of the service will make the service unavailable.

CVE ID: **CVE-2023-24511**
Severity: metric_v3 **HIGH**
Impact Score: metric_v3 **3.6**
URL: https://www.arista.com/en/support/advisories-notices/security-advisory/17239-security-advisory-0084
Description

> On affected platforms running Arista EOS with SNMP configured, a specially crafted packet can cause a memory leak in the snmpd process. This may result in the snmpd processing being terminated (causing SNMP requests to time out until snmpd is automatically restarted) and potential memory resource exhaustion for other processes on the switch. The vulnerability does not have any confidentiality or integrity impacts to the system.

CVE ID: **CVE-2023-24509**
Severity: metric_v3 **HIGH**
Impact Score: metric_v3 **5.9**
URL: https://www.arista.com/en/support/advisories-notices/security-advisory/16985-security-advisory-0082
Description

> On affected modular platforms running Arista EOS equipped with both redundant supervisor modules and having the redundancy protocol configured with RPR or SSO, an existing unprivileged user can login to the standby supervisor as a root user, leading to a privilege escalation. Valid user credentials are required in order to exploit this vulnerability.

CVE ID: **CVE-2023-24512**
Severity: metric_v3 **MEDIUM**
Impact Score: metric_v3 **3.6**
URL: https://www.arista.com/en/support/advisories-notices/security-advisory/17250-security-advisory-0086
Description

> On affected platforms running Arista EOS, an authorized attacker with permissions to perform gNMI requests could craft a request allowing it to update arbitrary configurations in the switch. This situation occurs only when the Streaming Telemetry Agent (referred to as the TerminAttr agent) is enabled and gNMI access is configured on the agent. Note: This gNMI over the Streaming Telemetry Agent scenario is mostly commonly used when streaming to a 3rd party system and is not used by default when streaming to CloudVision

CVE ID: **CVE-2023-24510**
Severity: metric_v3 **HIGH**
Impact Score: metric_v3 **3.6**
URL: https://www.arista.com/en/support/advisories-notices/security-advisory/17445-security-advisory-0087

Description

On the affected platforms running EOS, a malformed DHCP packet might cause the DHCP relay agent to restart.