IP FABRIC

COMMON VULNERABILITIES AND EXPOSURES (CVE)

for site **SITE 3 - Server Farm**

IP Fabric Common Vulnerabilities and Exposures (CVE) report generated with [ipfabric-reports] package at 2024-11-18_T09-35

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 for site SITE 3 - Server Farm

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
s3xdsw03	arista	eos	4.27.0F	10
s3xdsw04	arista	eos	4.27.0F	10
s3xgw2	arista	eos	4.27.0F	10
s3xasw01	arista	eos	4.27.0F	10
s3xdsw02	arista	eos	4.27.0F	10
s3xasw03	arista	eos	4.27.0F	10
s3xgw1	arista	eos	4.27.0F	10
s3xasw04	arista	eos	4.27.0F	10
d3xr01	cisco	ios	15.6(2)T	7
d3xr02	cisco	ios	15.6(2)T	7

2 Summary Vulnerability Analysis for site SITE 3 - Server Farm

Security Risk Overview

Total CVEs

114

Critical/High CVEs

70

Avg CVSS Score

7.09

Vulnerability Severity Distribution

Severity	Count	Percentage
CRITICAL	0	0.0%
HIGH	70	61.4%
MEDIUM	44	38.6%
LOW	0	0.0%

3 Detailed Vulnerability Analysis for site SITE 3 - Server Farm

ARISTA EOS (4.27.0F) Details

Affected Hostnames:

[s3xasw04, s3xdsw04, s3xasw03, s3xgw1, s3xdsw01, s3xdsw02, s3xgw2, s3xasw02, s3xasw01, 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.

CISCO IOS (15.6(2)T) Details

Affected Hostnames:

[d3xr02, d3xr01]

CVE List:

[CVE-2017-12289, CVE-2018-0167, CVE-2018-0175, CVE-2019-12655, CVE-2019-16009, CVE-2021-1460, CVE-2021-34703]

CVE Details:

CVE ID: **CVE-2017-12289**
Severity: metric_v3 **MEDIUM**
Impact Score: metric_v3 **3.6**
URL: http://www.securityfocus.com/bid/101509
Description

> A vulnerability in conditional, verbose debug logging for the IPsec feature of Cisco IOS XE Software could allow an authenticated, local attacker to display sensitive IPsec information in the system log file. The vulnerability is due to incorrect implementation of IPsec conditional, verbose debug logging that causes sensitive information to be written to the log file. This information should be restricted. An attacker who has valid administrative credentials could exploit this vulnerability by authenticating to the device and enabling conditional, verbose debug logging for IPsec and viewing the log file. An exploit could allow the attacker to access sensitive information related to the IPsec configuration. Cisco Bug IDs: CSCvf12081.

CVE ID: **CVE-2018-0167**
Severity: metric_v3 **HIGH**
Impact Score: metric_v3 **5.9**
URL: http://www.securityfocus.com/bid/103564
Description

> Multiple Buffer Overflow vulnerabilities in the Link Layer Discovery Protocol (LLDP) subsystem of Cisco IOS Software, Cisco IOS XE Software, and Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition or execute arbitrary code with elevated privileges on an affected device. Cisco Bug IDs: CSCuo17183, CSCvd73487.

CVE ID: **CVE-2018-0175**
Severity: metric_v3 **HIGH**
Impact Score: metric_v3 **5.9**
URL: http://www.securityfocus.com/bid/103564
Description

> Format String vulnerability in the Link Layer Discovery Protocol (LLDP) subsystem of Cisco IOS Software, Cisco IOS XE Software, and Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition or execute arbitrary code with elevated privileges on an affected device. Cisco Bug IDs: CSCvd73664.

CVE ID: **CVE-2019-12655**
Severity: metric_v3 **HIGH**
Impact Score: metric_v3 **3.6**
URL: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190925-ftp
Description

A vulnerability in the FTP application layer gateway (ALG) functionality used by Network Address Translation (NAT), NAT IPv6 to IPv4 (NAT64), and the Zone-Based Policy Firewall (ZBFW) in Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause an affected device to reload. The vulnerability is due to a buffer overflow that occurs when an affected device inspects certain FTP traffic. An attacker could exploit this vulnerability by performing a specific FTP transfer through the device. A successful exploit could allow the attacker to cause the device to reload.

CVE ID: **CVE-2019-16009**
Severity: metric_v3 **HIGH**
Impact Score: metric_v3 **5.9**
URL: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200108-ios-csrf
Description

A vulnerability in the web UI of Cisco IOS and Cisco IOS XE Software could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack on an affected system. The vulnerability is due to insufficient CSRF protections for the web UI on an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a malicious link. A successful exploit could allow the attacker to perform arbitrary actions with the privilege level of the targeted user. If the user has administrative privileges, the attacker could alter the configuration, execute commands, or reload an affected device.

CVE ID: **CVE-2021-1460**
Severity: metric_v3 **HIGH**
Impact Score: metric_v3 **3.6**
URL: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-dos-4Fgcjh6
Description

A vulnerability in the Cisco IOx Application Framework of Cisco 809 Industrial Integrated Services Routers (Industrial ISRs), Cisco 829 Industrial ISRs, Cisco CGR 1000 Compute Module, and Cisco IC3000 Industrial Compute Gateway could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient error handling during packet processing. An attacker could exploit this vulnerability by sending a high and sustained rate of crafted TCP traffic to the IOx web server on an affected device. A successful exploit could allow the attacker to cause the IOx web server to stop processing requests, resulting in a DoS condition.

CVE ID: **CVE-2021-34703**
Severity: metric_v3 **MEDIUM**
Impact Score: metric_v3 **3.6**
URL: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-lldp-dos-sBnuHSjT
Description

A vulnerability in the Link Layer Discovery Protocol (LLDP) message parser of Cisco IOS Software and Cisco IOS XE Software could allow an attacker to trigger a reload of an affected device, resulting in a denial of service (DoS) condition. This vulnerability is due to improper initialization of a buffer. An attacker could exploit this vulnerability via any of the following methods: An authenticated, remote attacker could access the LLDP neighbor table via either the CLI or SNMP while the device is in a specific state. An unauthenticated, adjacent attacker could corrupt the LLDP neighbor table by injecting specific LLDP frames into the network and then waiting for an administrator of the device or a network management system (NMS) managing the device to retrieve the LLDP neighbor table of the device via either the CLI or SNMP. An authenticated, adjacent attacker with SNMP read-only credentials or low privileges on the device CLI could corrupt the LLDP neighbor table by injecting specific LLDP frames into the network and then accessing the LLDP neighbor table via either the CLI or SNMP. A successful exploit could allow the attacker to cause the affected device to crash, resulting in a reload of the device.
