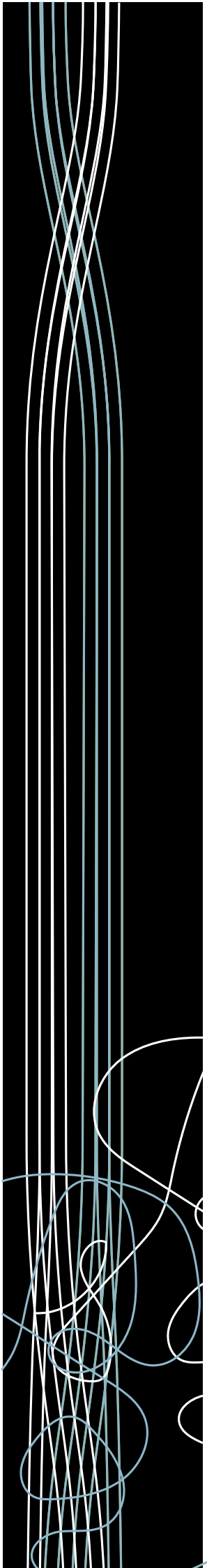


ORDR SECURITY BULLETIN

CISCO VULNERABILITIES

By: Pandian Gnanaprakasam

Coauthors: Srinivas Loke, Gowri Sunder Ravi

Contents

Introduction

Cisco has released **multiple security advisories impacting *multiple Cisco products*** where a remote threat actor could exploit vulnerabilities to take control of an affected system. This comes at the same time as a joint advisory covering ongoing threats to the firm's router firmware.

An advisory earlier this week from the NSA, FBI, CISA, and Japan's NISC security agency warned that a Chinese-linked threat group had been observed modifying firmware on Cisco routers to target US and Japanese organizations. The group, known as 'BlackTech', was found to have specifically targeted routers at divisional branch offices to gain a deeper foothold in corporate networks.

According to Cisco Talos, threat actors were observed using an older vulnerability, CVE-2021-1435, to install an implant after abusing CVE-2023-20198 to gain access to the device.

Impact

To help customers determine their exposure to vulnerabilities in Cisco IOS and IOS XE Software, Cisco provides the Cisco Software Checker. This tool identifies any Cisco security advisories that impact a specific software release and the earliest release that addresses the vulnerabilities described in each advisory (aka, *First Fixed*). If applicable, the tool returns the earliest release that addresses all the vulnerabilities described in all the advisories identified (aka, *Combined First Fixed*).

CVE	Security from Cisco Advisory	Product Affected	Versions
CVE-2023-20198	**Critical**	Cisco IOS Software / Cisco IOS XE Software	Exact versions not yet mentioned, this vulnerability affects Cisco IOS XE Software if the web UI feature is enabled. Cisco is aware of this CVE actively being exploited.
CVE-2023-20252	**Critical**	Cisco Catalyst SD-WAN Manager	20.9.4, 20.11
CVE-2023-20253	**High**	Cisco Catalyst SD-WAN Manager	20.6.2, 20.7.1, 20.8.1, 20.9.1, 20.10.11, 20.11.1
CVE-2023-20034	**High**	Cisco Catalyst SD-WAN Manager	20.3.4, 20.6.1, 20.7.1
CVE-2023-20254	**High**	Cisco Catalyst SD-WAN Manager	20.6.3.4, 20.9.3.2, 20.10.1.2, 20.11.1.2
CVE-2023-20262	**Medium**	Cisco Catalyst SD-WAN Manager	20.3.7, 20.9.3, 20.11.1, 20.12.1
CVE-2023-20231	**High**	Catalyst 9800-CL Wireless Controllers for Cloud Catalyst 9800 Embedded Wireless Controller for Catalyst 9300, 9400, and 9500 Series Switches	This vulnerability affects the following Cisco products if they run Cisco IOS XE Software, have a Lobby Ambassador account enabled, and have the HTTP server feature enabled.

		Embedded Wireless Controller on Catalyst 9100X Series Access Points	
CVE-2023-20187	**Critical**	Cisco ASR 1000 Series Aggregation Service Routers	The exact version is not mentioned. It is affected if devices satisfy all the mentioned in the advisory. (cisco-sa-mlre-H93FswRz)
CVE-2023-20227	**High**	1000,1100,4000 Series Integrated Services Routers Catalyst 8000V Edge Software Catalyst 8200,8300,8500L Series Edge Platforms Cloud Services Routers 1000V Series Integrated Services Virtual Routers VG400, VG420, VG450 Analog Voice Gateways	The exact version is not mentioned. It is affected if devices have an L2TP feature with active tunnels.
CVE-2023-20223	**High**	Cisco DNA Center deployments	The exact version is not mentioned. All deployments that have disaster recovery enabled.
CVE-2023-20033	**High**	Catalyst 3650, 3850 Series Switches	Affected if running Cisco IOS XE Software and having a management interface enabled.
CVE-2023-20226	**High**	4200, 4300 Series Integrated Services Routers Catalyst 8000V Edge Software Catalyst 8200,8300,8500L Series Edge Platforms Catalyst IR8300 Rugged Series Routers ISR1100 Series Routers	The exact version is not mentioned. It is affected if the device is running Cisco IOS XE Software and has AppQoE or UTD enabled.
CVE-2023-20186	**High**	Cisco IOS Software / Cisco IOS XE Software	The exact version is not mentioned. It is affected if devices have SCP server functionality and AAA command authorization enabled.
CVE-2023-20101	**Critical**	Cisco Emergency responder	This vulnerability affects only Cisco Emergency Responder Release 12.5(1)SU4.
CVE-2023-20259	**High**	Emergency Responder Prime Collaboration Deployment Unified Communications Manager (Unified CM) Unified Communications Manager IM & Presence Service (Unified CM IM&P) Unified Communications Manager Session Management Edition (Unified CM SME) Unity Connection	This vulnerability affects the following Cisco products independent of device configuration.
CVE-2023-20235	**Medium**	Catalyst IE3x00 Rugged Series Switches Catalyst IR1100, IR1800, IR8100, IR8300 Rugged Series Routers	Running a vulnerable release of Cisco IOS XE Software (17.3.1 and later) was configured with the Cisco IOx application hosting environment and

		Embedded Services 3300 Series Switches	enabled the application development workflow feature.

Vulnerability Details

1. **Cisco IOS XE Software Web UI Privilege Escalation Vulnerability**

   - CVE-2023-20198: is a privilege escalation vulnerability affecting Cisco IOS XE software. The vulnerability has a maximum severity CVSS score of 10.
   - Successful exploitation of this vulnerability would allow an attacker to create a user account with full administrative privileges. The vulnerability lies within the Web UI feature of the software.
   - This vulnerability affects Cisco IOS XE Software if the web UI feature is enabled. The web UI feature is enabled through the **ip http server** or **ip http secure-server** commands.

2. **Cisco Catalyst SD-WAN Manager Vulnerabilities**

   - CVE-2023-20034: is a high-severity vulnerability that could allow an unauthorized, remote attacker to access sensitive data from the Elasticsearch database.
   - CVE-2023-20252: is a critical-severity vulnerability in the SAML APIs that could allow an unauthenticated, remote attacker to gain unauthorized access to the application.
   - CVE-2023-20253: is a high-severity vulnerability in the command line interface (CLI) management interface. It could allow an authenticated, local attacker with read-only privileges to bypass authorization and roll back controller configurations, which could be deployed to downstream routers.
   - CVE-2023-20254: is a high-severity vulnerability in the session management system. It could allow an authenticated, remote attacker to access another tenant managed by the same instance.
   - CVE-2023-20262: is a medium-severity vulnerability in the SSH service. It could allow an unauthenticated, remote attacker to cause a process crash, resulting in a DoS condition for SSH access.

3. **Cisco IOS XE Software Web UI Command Injection Vulnerability**:

   - CVE-2023-20231: is a high-severity vulnerability that could allow an authenticated, remote attacker to perform an injection attack against an affected device. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to execute arbitrary CLI commands with level 15 privileges.

4. **Cisco IOS XE Software for ASR 1000 Series Aggregation Services Routers IPv6 Multicast Denial of Service Vulnerability:**

   - CVE-2023-20187: is a critical vulnerability in the Multicast Leaf Recycle Elimination (mLRE) feature. It could allow an unauthenticated, remote attacker to cause the affected device to reload, resulting in a DoS condition.

5. **Cisco IOS XE Software Layer 2 Tunneling Protocol Denial of Service Vulnerability**:

   - **CVE-2023-20227**: is a high-severity vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper handling of certain L2TP packets. An attacker could exploit this vulnerability by sending crafted L2TP packets to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly, resulting in a DoS condition.

     Note: *Only traffic directed to the affected system can be used to exploit this vulnerability.*

6. **Cisco DNA Center API Insufficient Access Control Vulnerability**:

   - **CVE-2023-20223**: is a high-severity vulnerability in Cisco IOS XE Software that could allow an unauthenticated, remote attacker to cause an affected device to reload, resulting in a denial of service (DoS) condition. This vulnerability is due to buffer exhaustion while processing traffic on a configured IPsec tunnel. An attacker could exploit this vulnerability by sending traffic to an affected device with a maximum transmission unit (MTU) of 1800 bytes or greater. A successful exploit could allow the attacker to cause the device to reload.

7. **Cisco IOS XE Software for Catalyst 3650 and Catalyst 3850 Series Switches Denial of Service Vulnerability**:

   - **CVE-2023-20033**: is a high-severity vulnerability in Cisco IOS XE Software for Cisco Catalyst 3650 and Catalyst 3850 Series Switches. This vulnerability could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition.

8. **Cisco IOS XE Software Application Quality of Experience and Unified Threat Defense Denial of Service Vulnerability**:

   - **CVE-2023-20226**: is a high-severity vulnerability that could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a DoS condition.

9. **Cisco IOS and IOS XE Software Command Authorization Bypass Vulnerability:**

   - **CVE-2023-20186**: is a high-severity vulnerability in the AAA feature of Cisco IOS Software and Cisco IOS XE Software. It could allow an authenticated, remote attacker to bypass command authorization and copy files to or from the file system of an affected device using the Secure Copy Protocol (SCP).

10. **Cisco Emergency Responder Static Credentials Vulnerability:**

    - **CVE-2023-20101**: is a critical severity vulnerability that allows an unauthenticated, remote attacker to log in to an affected device using the root account, which has default, static credentials that cannot be changed or deleted. The root account serves for use during development. An attacker could exploit this vulnerability by logging into an affected system using the account. A successful exploit could allow the attacker to log into the affected system and execute arbitrary commands as the root user.

11. **Multiple Cisco Unified Communications Products Unauthenticated API High CPU Utilization Denial of Service Vulnerability:**

    - CVE-2023-20259: is a high-severity vulnerability in an API endpoint that could allow an unauthenticated, remote attacker to cause high CPU utilization, impacting access to the web-based management interface and causing delays with call processing.

12. **Cisco IOx Application Hosting Environment Privilege Escalation Vulnerability:**

    - CVE-2023-20235: is a medium severity vulnerability found in specific Cisco IOS XE Software versions. This vulnerability could allow an authenticated, remote attacker to access the underlying operating system as the root user. The issue exists because the application development mode does not block Docker containers with the privileged runtime option. An attacker could exploit this vulnerability by using the Docker CLI to access an affected device. Users should use the application development workflow only on development systems, not production systems.

Organizations strongly advise applying the patches from Cisco as soon as possible to mitigate the risk associated with these vulnerabilities.

How Ordr Helps

Locate Vulnerable Devices

- Ordr automatically discovers and classifies all devices based on the manufacturer, make, and model.
- Ordr provides filters to help quickly identify affected Cisco devices in an environment.

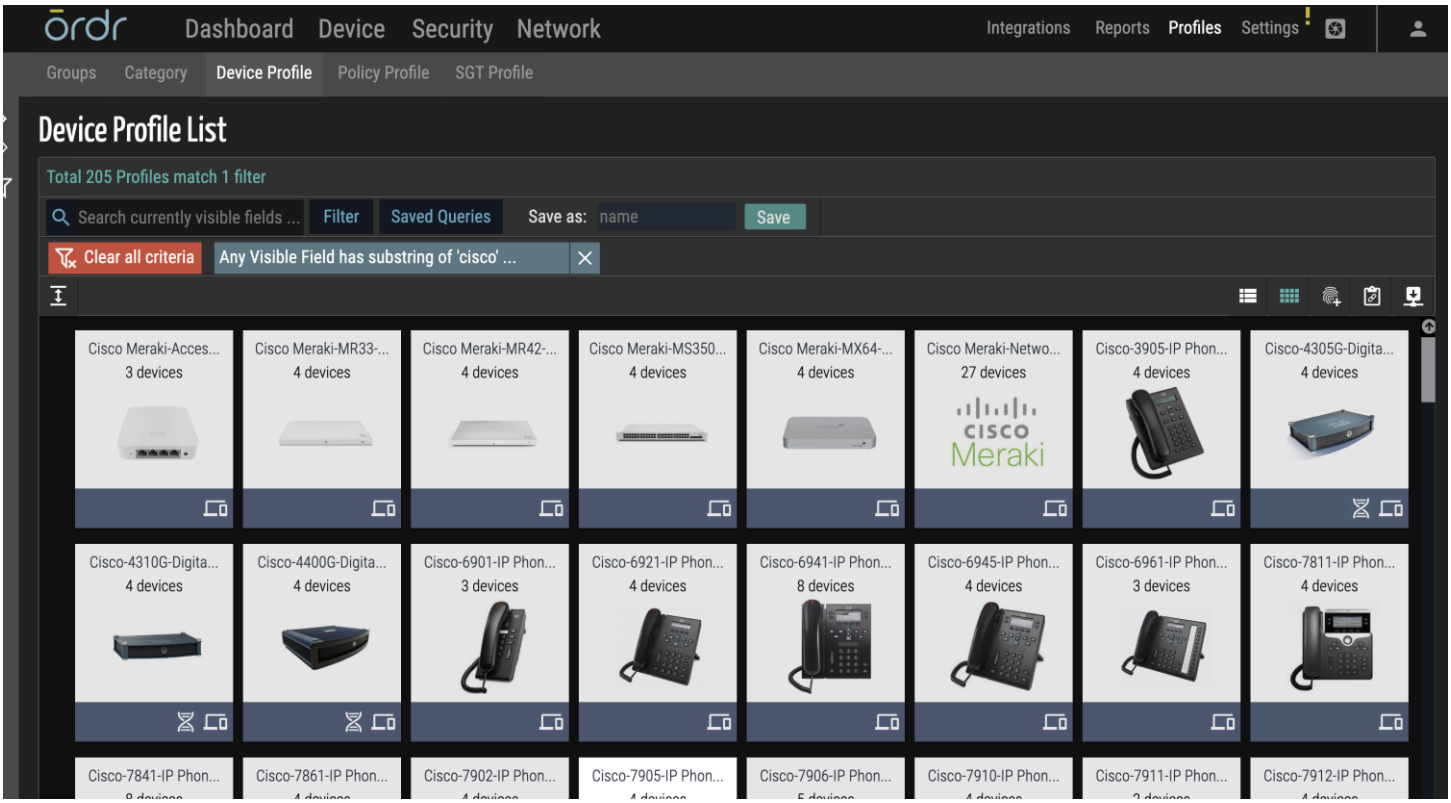


Figure 1: Device Profile List

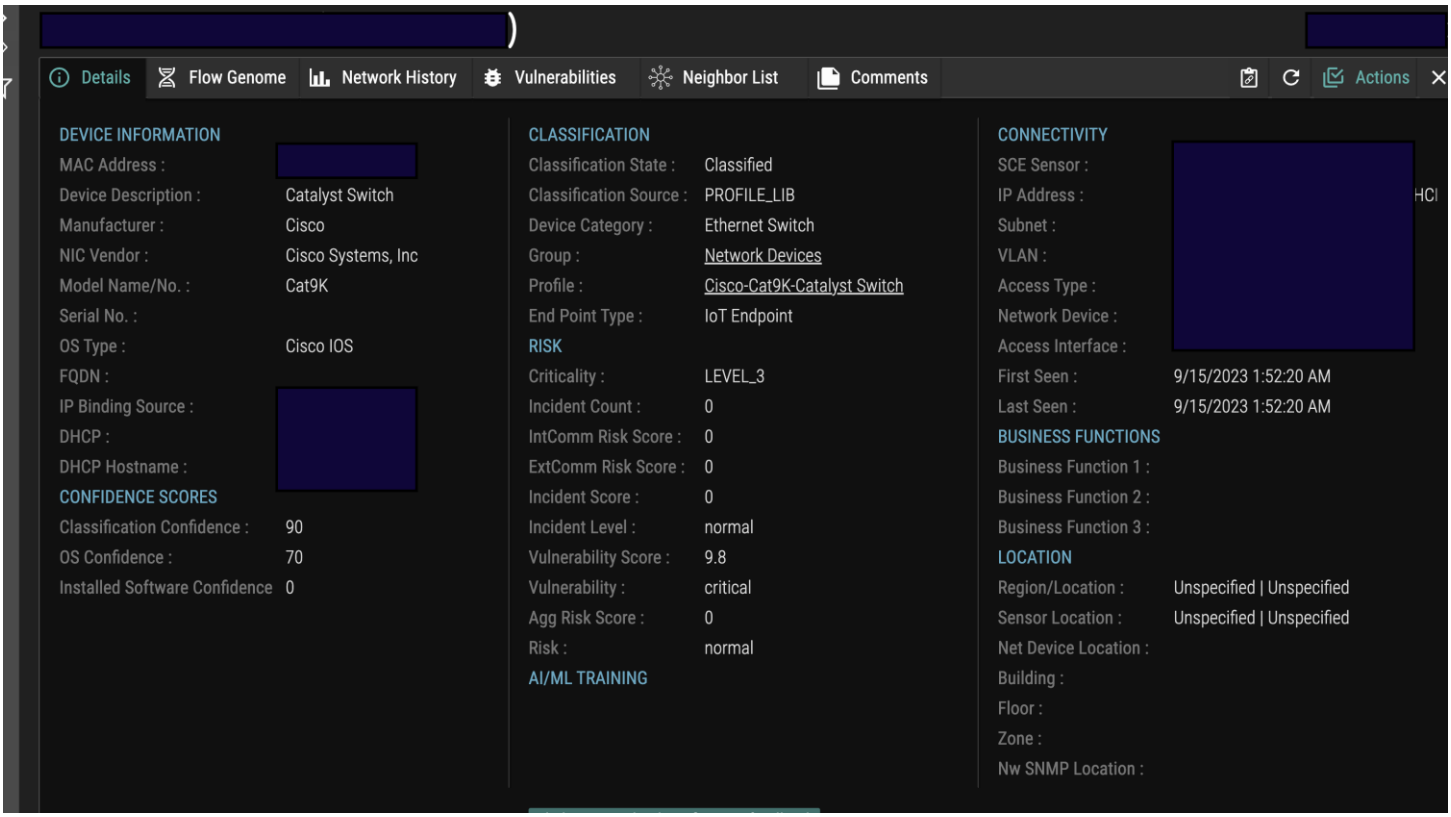


Figure 2: Device Details

Vulnerability Mapping of Impacted Devices

- *Ordr Software Inventory Collector* provides application mapping, and the *Ordr Vulnerability Matching Engine* identifies if your organization is impacted.
- *Ordr Software Inventory* Collector can be deployed on an endpoint (e.g., device, workstation, or server) to provide visibility into installed applications on that endpoint.
- Ordr maintains a list of all the software packages installed on each endpoint, including version numbers and timestamps indicating when they were installed or last updated.
- *Ordr Vulnerability Mapping Engine* assigns vulnerabilities based on the Software Version (SW) version collected from the endpoint. The installed application list is updated daily, and vulnerabilities are recalculated based on the new info. The *Ordr Vulnerability Database* can be used to identify vulnerable Cisco devices.

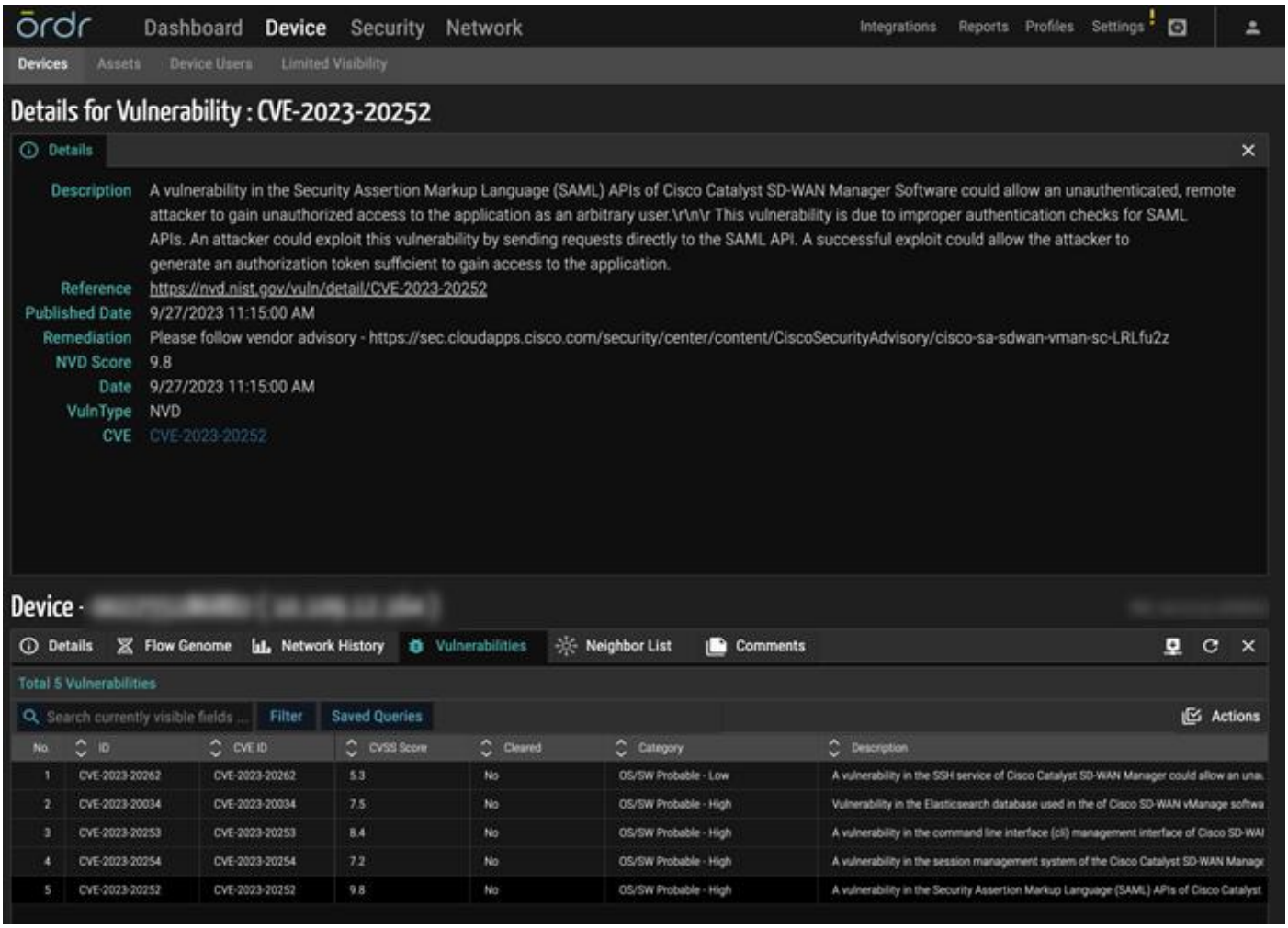


Figure 3: Details for Vulnerability

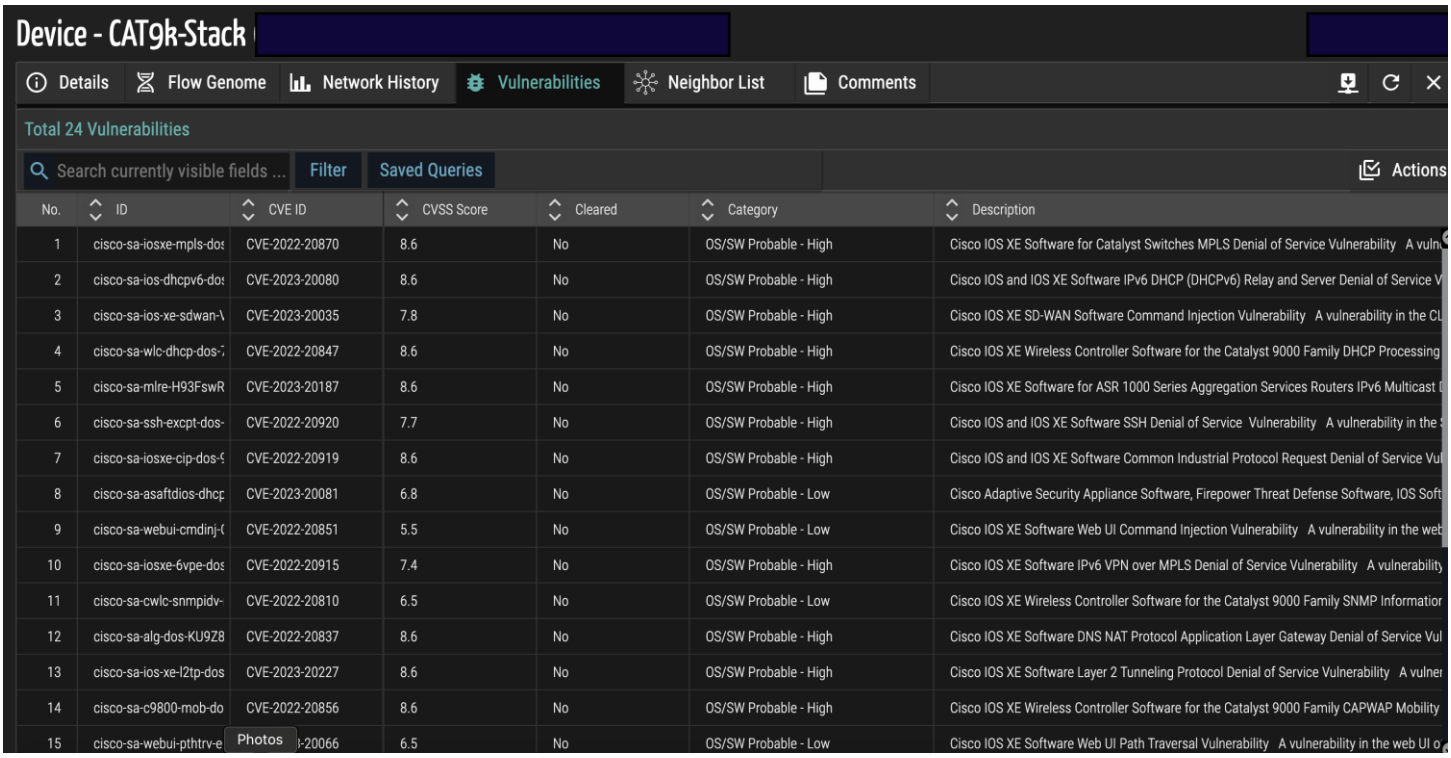


Figure 4: List of Vulnerabilities

Integration with Vulnerability Response Systems

- Ordr provides a centralized view of Cisco vulnerabilities and corresponding details for all connected devices by combining data from multiple sources with the help of vulnerability response systems such as ServiceNow Vulnerability Response to optimize prioritization, assignment/ticketing, and management of vulnerabilities across the entire lifecycle.

Network Segmentation

- Ordr segmentation policies can protect vulnerable mission-critical devices that must stay in operation by restricting device communications to reduce the attack surface.
- Ordr segmentation policies are enforced through integrations with multiple industry-leading security and network vendors.

Baseline Communications to Identify Malicious Anomalies

- Ordr uses AI/ML to create a baseline of normal communications for each device based on profile, location, business function, or any customized entity.
- Ordr can trigger alerts based on any observed deviations from the device baseline when anomalies are detected.
- Ordr also recommends using our behavioral anomaly and threat detection capabilities to identify anomalies during any incident response or remediation effort.
- Ordr calculates and adjusts the risk score of each device based on the events detected in addition to asset criticality. All device risk scores are normalized based on the criticality.

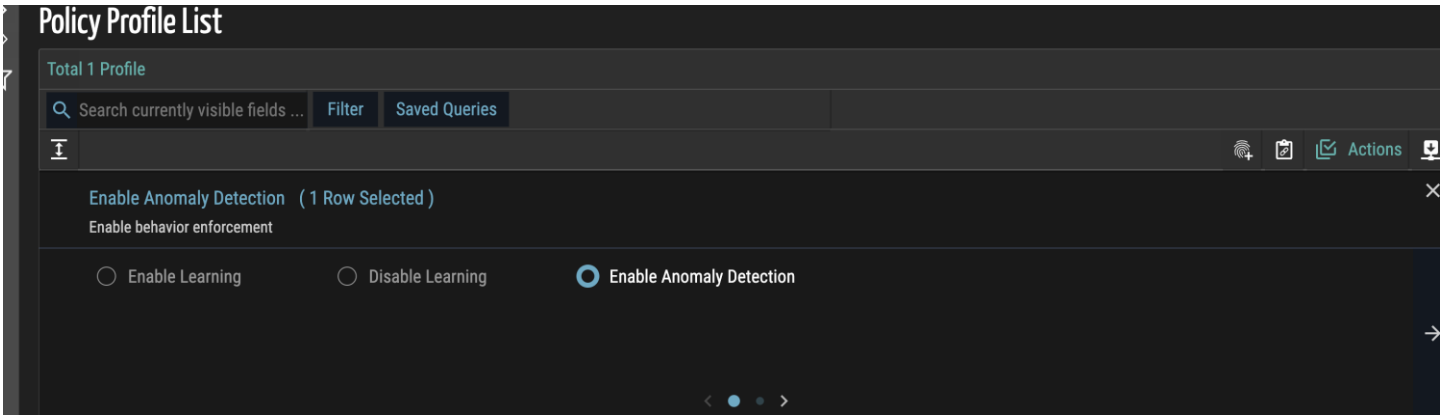


Figure 5: Enable Anomaly Detection

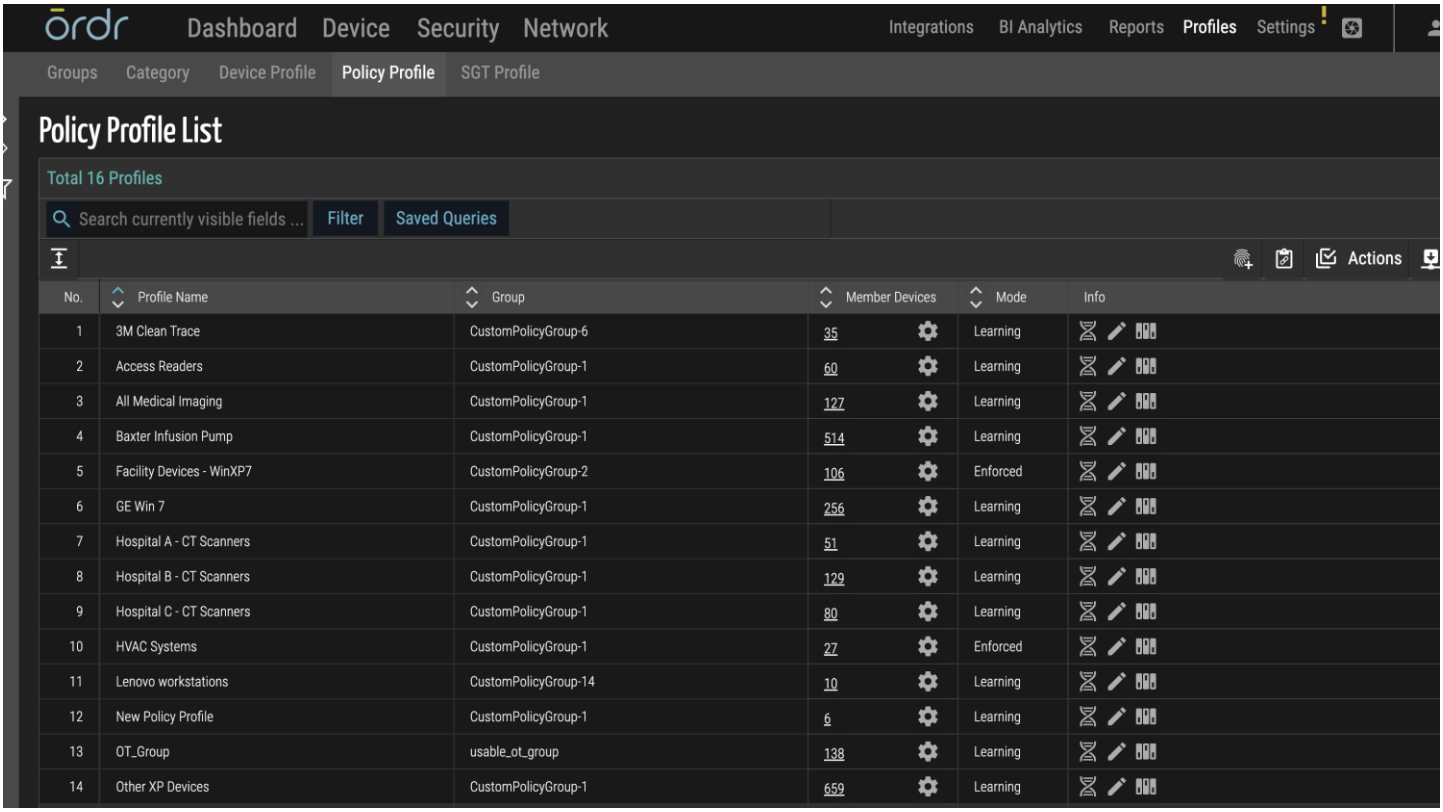


Figure 6: Policy Profile List

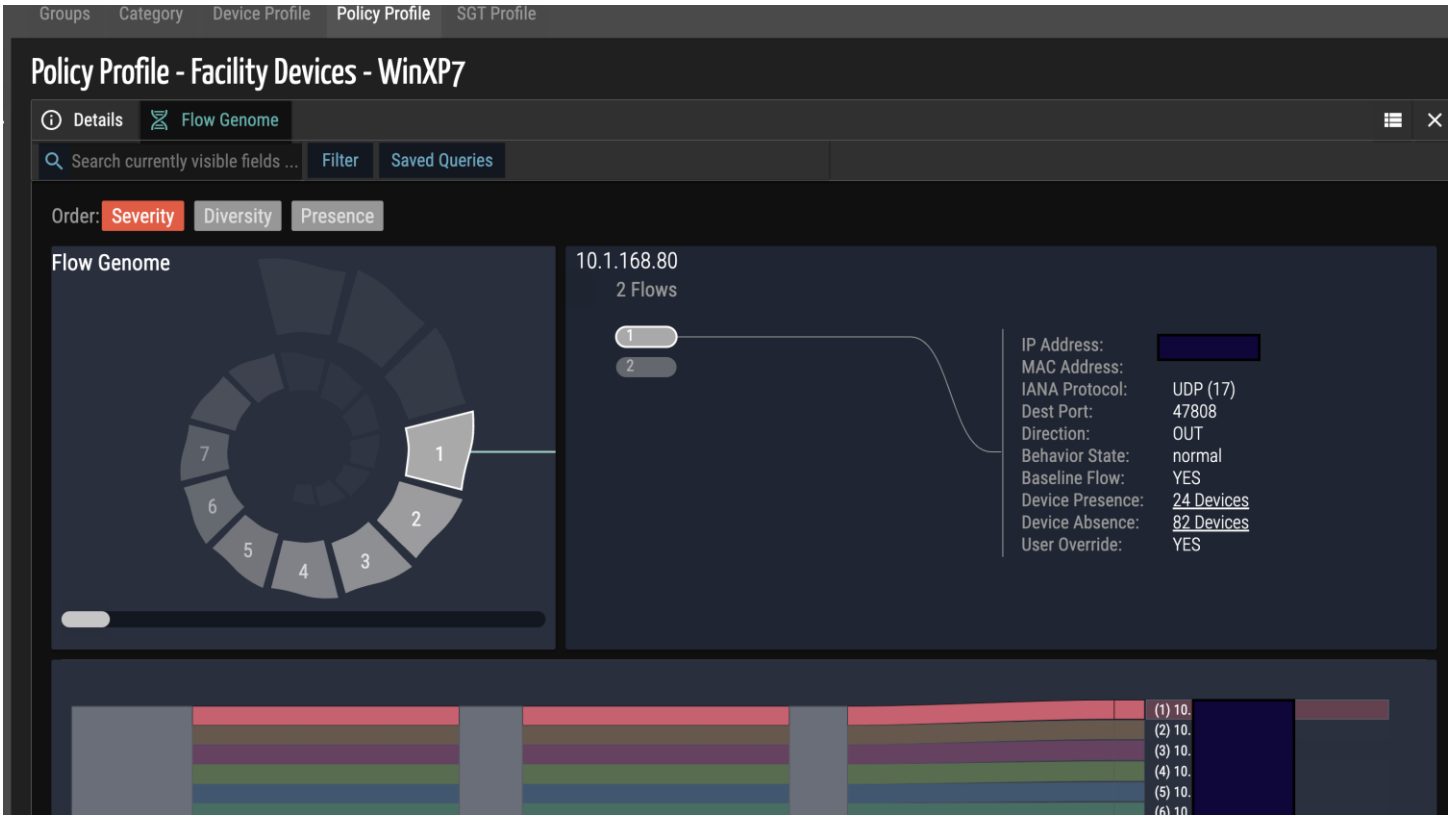


Figure 7: Flow Genome

Proactive Firewall Policies

- Ordr allows you to create a policy profile that includes all affected devices and build a firewall policy to block communications from one or more external addresses.
- Ordr policy is enforced through integration with multiple industry-leading firewall vendors.

No.	Name	Logo	Category
1	Check Point	CHECK POINT	Firewall
2	Cisco Firepower	cisco	Firewall
3	Fortinet	FORTINET	Firewall
4	Meraki	cisco Meraki	Firewall
5	Palo Alto Networks	paloalto NETWORKS	Firewall

Figure 8: Firewalls

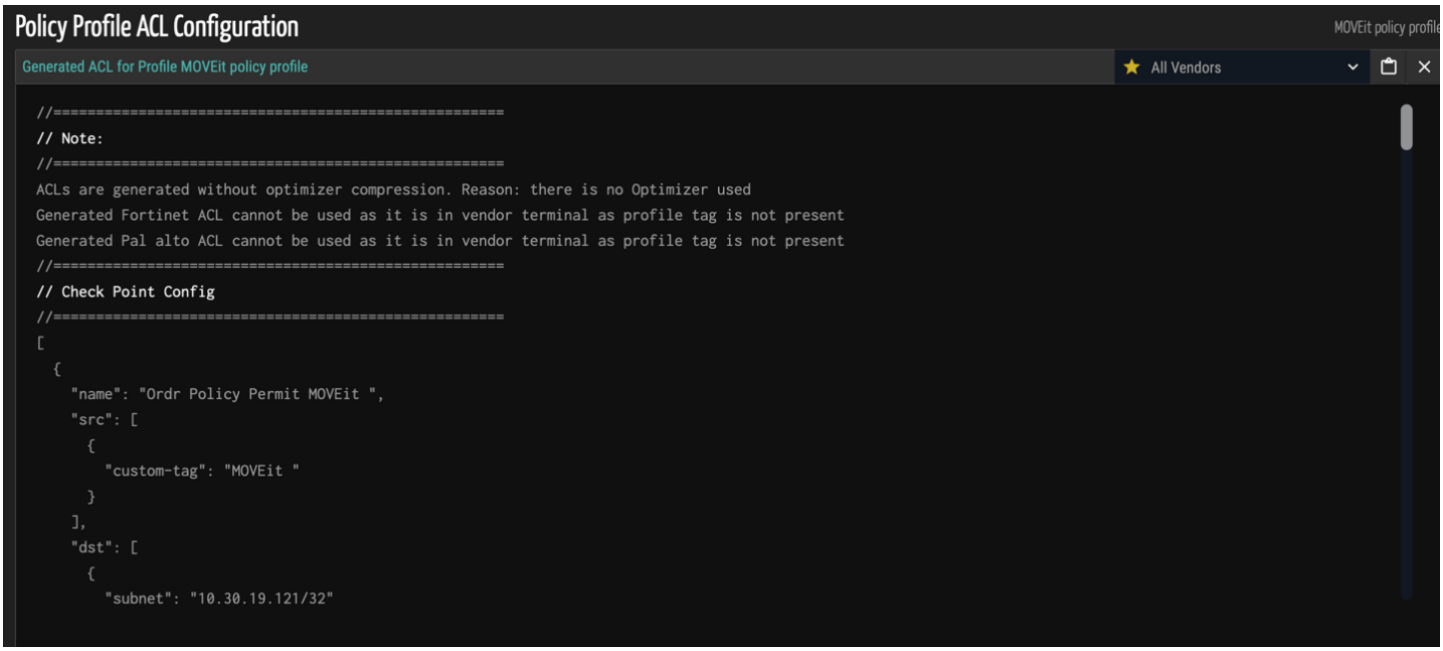


Figure 9: Check Point Configuration

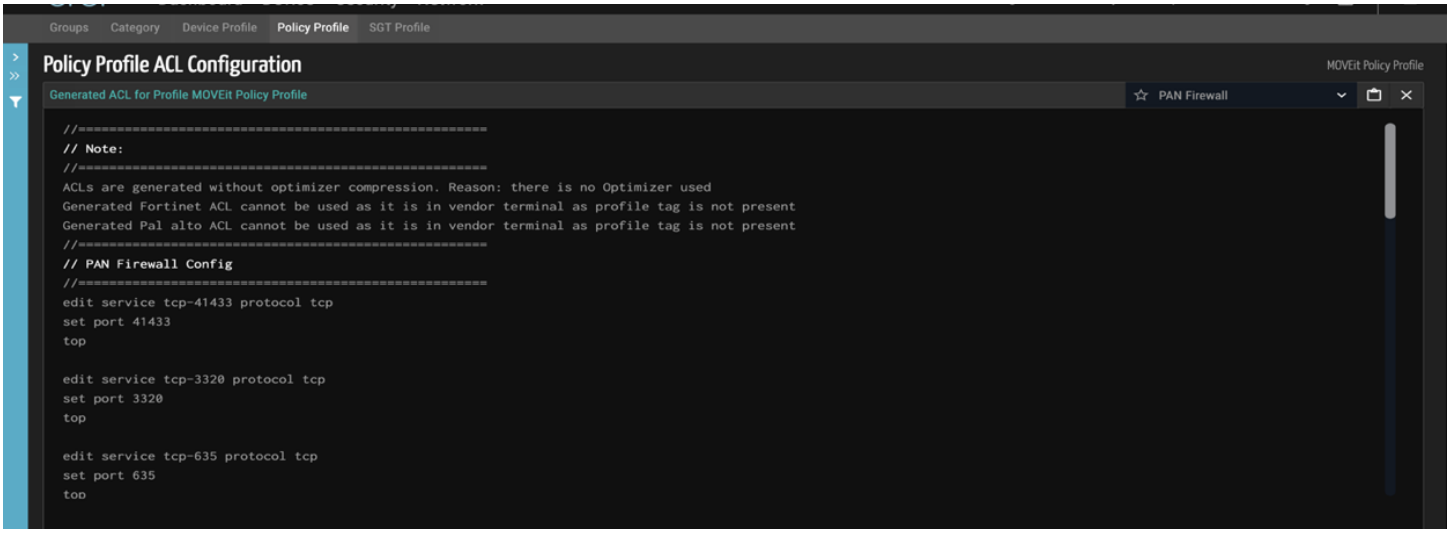


Figure 10: PAN Firewall Configuration

Remediation and Mitigation

Customers can use Cisco Software Checker to determine if vulnerabilities impact deployed software versions.

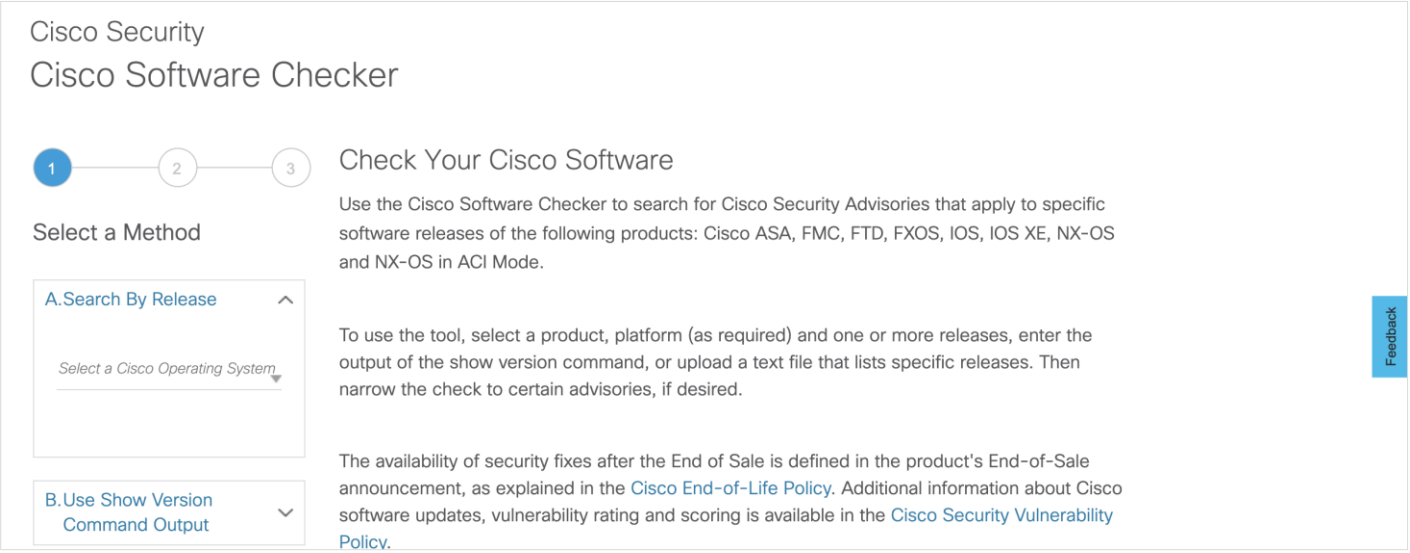


Figure 11: Cisco Software Checker

Update Software to the Latest Version for All Impacted Products

- It is recommended to apply the necessary updates provided by Cisco as soon as possible to address vulnerabilities and prevent exploitation.

Rapid Threat Containment if a Breach is Detected

- Ordr tracks the connectivity of every device and maintains real-time data on the device's connection within the enterprise network – whether connected to a wired switch, wireless AP, VPN, or any other network component.
- When an active threat is detected, Ordr provides incident response teams with one-click actions to isolate (e.g., move to a quarantine VLAN) or segment impacted devices.
- Ordr supports a variety of threat containment actions, as shown below:

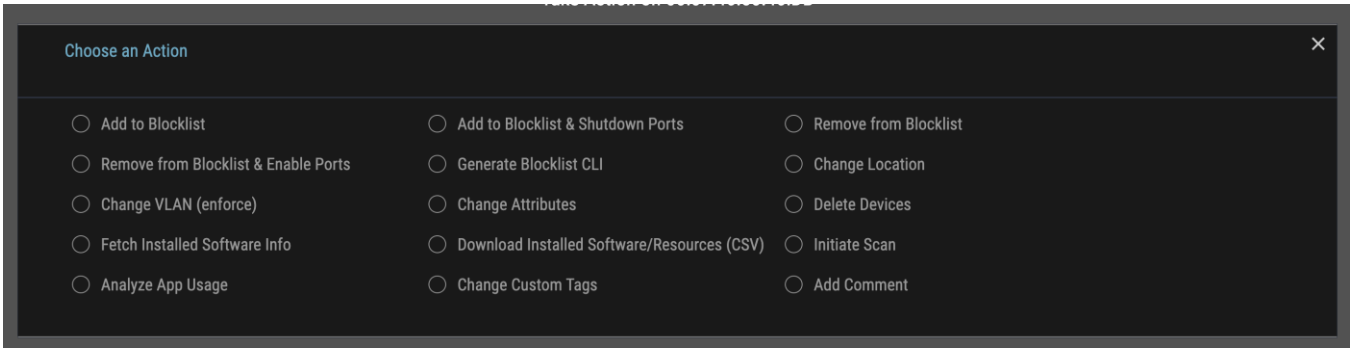
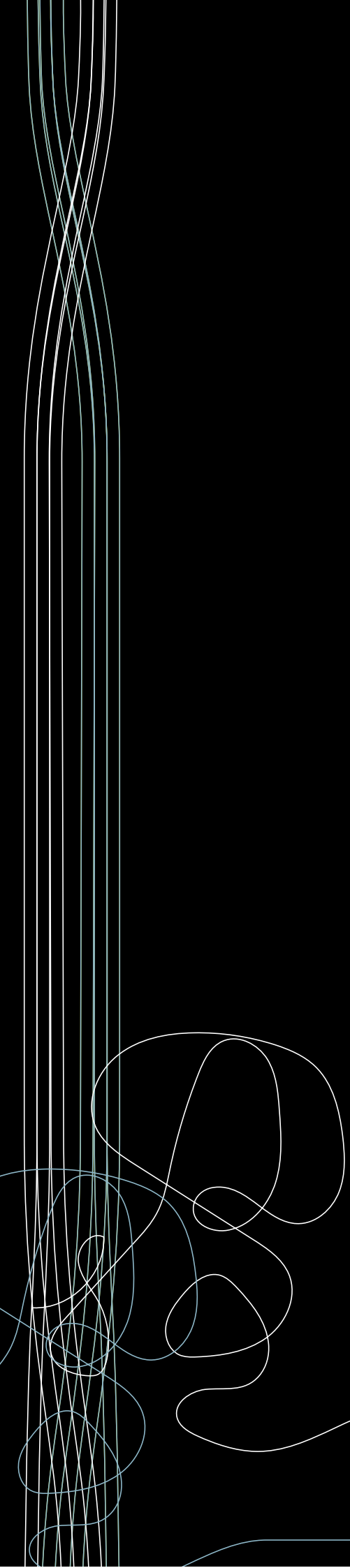


Figure 12: Choose an Action

For specific details about each vulnerability, including remediation and mitigation actions, please refer to the specific advisory provided by Cisco for each CVE.

Helpful Links

1. Cisco Catalyst SD-WAN Manager Vulnerabilities: cisco-sa-sdwan-vman-sc-LRLfu2z
2. Cisco IOS XE Software Web UI Command Injection Vulnerability: cisco-sa-webui-cmdij-FzZAeXAy
3. Cisco IOS XE Software for ASR 1000 Series Aggregation Services Routers IPv6 Multicast Denial of Service Vulnerability: cisco-sa-mlre-H93FswRz
4. Cisco IOS XE Software Layer 2 Tunneling Protocol Denial of Service Vulnerability: cisco-sa-ios-xe-l2tp-dos-eB5tuFmV
5. Cisco DNA Center API Insufficient Access Control Vulnerability: cisco-sa-dnac-ins-acc-con-nHAVDRBZ
6. Cisco IOS XE Software for Catalyst 3650 and Catalyst 3850 Series Switches Denial of Service Vulnerability: cisco-sa-cat3k-dos-ZZA4Gb3r
7. Cisco IOS XE Software Application Quality of Experience and Unified Threat Defense Denial of Service Vulnerability: cisco-sa-appqoe-utd-dos-p8O57p5y
8. Cisco IOS and IOS XE Software Command Authorization Bypass Vulnerability: cisco-sa-aaascp-Tyj4fEJm
9. CISA advisory related to black tech group: https://www.cisa.gov/news-events/alerts/2023/09/27/nsa-fbi-cisa-and-japanese-partners-release-advisory-prc-linked-cyber-actors
10. Cisco Software Checker
11. https://www.scmagazine.com/news/blacktech-gang-hacks-cisco-firmware-in-attacks-on-multinational-corporations
12. https://ordr.net/
13. https://blog.talosintelligence.com/active-exploitation-of-cisco-ios-xe-software/
14. https://www.darkreading.com/vulnerabilities-threats/critical-unpatched-cisco-zero-day-bug-active-exploit



ōrdr

info@ordr.net
www.ordr.net

2445 Augustine Drive Suite 601
Santa Clara, CA 95054