August 18, 2023

Overall rating: High

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of multiple Cisco vulnerabilities. There are numerous vulnerabilities, impacting multiple Cisco applications and devices detailed in the Cisco references below, VRM recommends reviewing the notifications and CVEs detailing the vulnerabilities, mitigations, and links to updates for your organizational systems.

Technical Details

Application	Impact	Vulnerability	Affected Products	Risk	CVE
Cisco ThousandEyes Enterprise Agent Virtual Appliance Privilege Escalation Vulnerability	May allow the attacker to execute arbitrary commands as root. The attacker must have valid credentials on the affected device.	Privilege Escalation	Virtual Appliance installation of Cisco ThousandEyes Enterprise Agent	**HIGH**	CVE-2023-20224
Cisco ThousandEyes Enterprise Agent Virtual Appliance	May an authenticated, local attacker to elevate privileges on an affected device.	Privilege Escalation	Virtual Appliance installation of Cisco ThousandEyes Enterprise Agent	**MEDIUM**	CVE-2023-20217
Cisco Integrated Management Controller	May allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface.	Cross-Site Scripting	Vulnerable release of Cisco IMC: • 5000 Series Enterprise Network Compute System (ENCS) • UCS C-Series M5 and previous generation Rack Servers • UCS E-Series M3 Servers	**MEDIUM**	CVE-2023-20228
Cisco Duo Device Health Application for Windows	May allow an authenticated, local attacker with low privileges to conduct directory traversal attacks and overwrite arbitrary files on an affected system.	Arbitrary File Write	Cisco Duo Device Health Application for Windows	**HIGH**	CVE-2023-20229
Cisco Unified Communications Manager	May allow an authenticated, remote attacker to conduct SQL injection attacks on an affected system.	SQL Injection	Cisco Unified CM and Cisco Unified CM SME	**HIGH**	CVE-2023-20211
ClamAV HFS+	May allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device.	Denial of Service	Affected Cisco Software Platform • Secure Endpoint Connector for Linux • Secure Endpoint Connector for MacOS • Secure Endpoint Connector for Windows	**HIGH**	CVE-2023-20197

			• Secure Endpoint Private Cloud		
ClamAV AutoIt Module	May allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device.	Denial of Service	Affected Cisco Software Platform • Secure Endpoint Connector for Windows • Secure Endpoint Private Cloud	**HIGH**	CVE-2023-20212
Cisco Unified Contact Center Express	May allow an unauthenticated, remote attacker to cause a web cache poisoning attack on an affected device.	Web Cache Poisoning	Cisco Unified CCX Finesse Portal	**MEDIUM**	CVE-2023-20232
Cisco Prime Infrastructure and Evolved Programmable Network Manager	May allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface on an affected device.	Cross-Site Scripting	Cisco Prime Infrastructure and Cisco EPNM	**MEDIUM**	CVE-2023-20222
Cisco Prime Infrastructure and Evolved Programmable Network Manager	May allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface on an affected device.	Cross-Site Scripting	Cisco Prime Infrastructure and Cisco EPNM	**MEDIUM**	CVE-2023-20201 CVE-2023-20203 CVE-2023-20205
Cisco Intersight Private Virtual Appliance	May allow an authenticated, remote attacker to execute arbitrary commands using root-level privileges. The attacker would need to have Administrator privileges on the affected device to exploit these vulnerabilities.	Command Injection	Cisco Intersight Private Virtual Appliance	**MEDIUM**	CVE-2023-20013 CVE-2023-20017
Cisco Identity Services Engine	May allow an authenticated, remote attacker to access sensitive information.	Information Disclosure	Cisco ISE	**MEDIUM**	CVE-2023-20111
Cisco IP Phone 6800, 7800, and 8800 Series	May allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack against a user of the web-based management interface of an affected system.	Cross-Site Request Forgery	Cisco products if they were running a vulnerable release of Multiplatform Firmware: • IP Phone 6800 Series with Multiplatform Firmware • IP Phone 7800 Series with Multiplatform Firmware • IP Phone 8800 Series with Multiplatform Firmware • Video Phone 8875	**MEDIUM**	CVE-2023-20221
Cisco Intersight Virtual Appliance	May allow an unauthenticated, adjacent attacker to access internal HTTP services that are otherwise inaccessible.	Unauthenticated Port Forwarding	Cisco Intersight Software: • Intersight Assist • Intersight Connected Virtual Appliance • Intersight Private Virtual Appliance	**MEDIUM**	CVE-2023-20237
Cisco Expressway Series and Cisco TelePresence Video Communication Server	May allow an authenticated, remote attacker with read-write privileges on the application to perform a command injection attack that could result in remote code execution on an affected device.	Command Injection	Cisco Expressway Series and Cisco TelePresence VCS if they were running a vulnerable release and had the Automatic Certification Revocation Lists (CRL) updates feature enabled.	**MEDIUM**	CVE-2023-20209

Cisco Unified Communications Products	May allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface.	Cross-Site Scripting	Cisco products: • Unified CM • Unified CM SME • Unified CM IM&P	**MEDIUM**	CVE-2023-20242
Cisco Secure Web Appliance	May allow an unauthenticated, remote attacker to bypass a configured rule, allowing traffic onto a network that should have been blocked.	Content Encoding Filter Bypass	Cisco Secure Web Appliance, both virtual and hardware versions, when the deflate, lzma, or brotli content-encoding type was enabled.	**MEDIUM**	CVE-2023-20215
Cisco Unified Communications Products	May allow an authenticated, remote attacker to read arbitrary files from the underlying operating system.	Arbitrary File Read	Cisco Unified CM and Unified CM SME	**MEDIUM**	CVE-2022-20790
Cisco BroadWorks CommPilot Application Software	May allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface.	Cross-Site Scripting	Cisco products: • BroadWorks Application Delivery Platform • BroadWorks Application Server (AS) • BroadWorks Xtended Services Platform (XSP)	**MEDIUM**	CVE-2023-20204
Cisco BroadWorks	May allow an authenticated, local attacker to elevate privileges to root on an affected system.	Privilege Escalation	Cisco products if they were running a vulnerable release of Cisco BroadWorks Software: • BroadWorks Application Delivery Platform • BroadWorks Application Server • BroadWorks Database Server • BroadWorks Database Troubleshooting Server • BroadWorks Execution Server • BroadWorks Media Server • BroadWorks Messaging Server • BroadWorks Network Database Server • BroadWorks Network Function Manager • BroadWorks Network Server • BroadWorks Profile Server • BroadWorks Service Control Function Server • BroadWorks Sharing Server • BroadWorks Video Server • BroadWorks WebRTC Server • BroadWorks Xtended Services Platform	**HIGH**	CVE-2023-20216

These vulnerabilities are rated from **HIGH** to **MEDIUM** risks. Software patches exists to address these risks.

Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

Please notify VRM with any questions or concerns you may have.

References

- Cisco Security Advisories