Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Cisco Small Business Routers Vulnerable to Authentication Bypass and Remote Code Execution

Date of Publication

January 16, 2023

Admiralty Code

A1

TA Number

TA2023025

Summary

First Seen: January 11, 2022
Affected Product: Cisco Small Business Routers
Impact: A remote attacker bypasses authentication or execute arbitrary commands on the underlying operating system of an affected device

CVEs

CVE	NAME	PATCH
CVE-2023-20025	Authentication Bypass Vulnerability	⊗
CVE-2023-20026	Remote Command Execution Vulnerability	⊗

Vulnerability Details

Multiple vulnerabilities were found in the web-based management interface of Cisco Small Business Routers. The authentication bypass vulnerability (CVE-2023-20025) allows an unauthenticated attacker to bypass authentication on an affected device by manipulating user input in incoming HTTP packets. The remote code execution vulnerability (CVE-2023-20026) allows an authenticated attacker to execute arbitrary commands on an affected device by manipulating user input in incoming HTTP packets. As these routers have reached the end of life, no software updates or workarounds are available to address these vulnerabilities. However, as proof-of-concept (PoC) is available, it is recommended to mitigate these vulnerabilities by blocking ports 443 and 60443 and disabling remote management.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-20025	Cisco RV Series Small Business Routers: RV016 Multi-WAN VPN Routers RV042 Dual WAN VPN Routers RV042G Dual Gigabit WAN VPN Routers RV082 Dual WAN VPN Routers	cpe:2.3:h:cisco:rv016_multi-wan_vpn_router:-:*:*:*:*:*:*:* cpe:2.3:h:cisco:rv042_dual_wan_vpn_router:-:*:*:*:*:*:*:* cpe:2.3:h:cisco:rv042g_dual_gigabit_wan_vpn_router:-:*:*:*:*:*:*:* cpe:2.3:h:cisco:rv082_dual_wan_vpn_router:-:*:*:*:*:*:*:*	CWE-287
CVE-2023-20026			CWE-78

Recommendations

Security Leaders

Asset and vulnerability management solutions should be implemented to ensure that all internet-accessible devices are secure, patched, updated, hardened, and monitored. Integrate and communicate all lessons learned.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize the vulnerability, identify the impacted assets, and patch them through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.
- **All Engineers:** Refer to and action upon the 'Potential MITRE ATT&CK TTPs' on the following pages.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	T1078 Valid Accounts	T1059 Command and Scripting Interpreter	T1098 Account Manipulation
T1203 Exploitation for Client Execution	T1068 Exploitation for Privilege Escalation	T1574 Hijack Execution Flow	

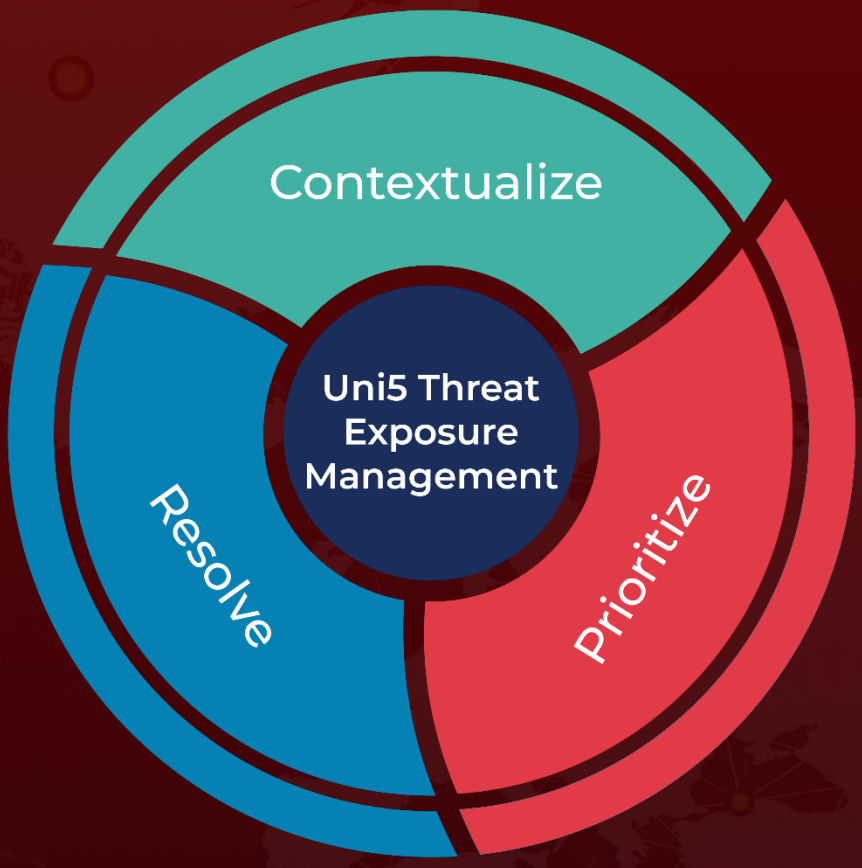
References

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sbr042-multi-vuln-ej76Pke5

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

January 16, 2023 • 3:40 AM

More at www.hivepro.com