Hive Pro

THREAT ADVISORY

Critical flaws in Cisco's Small Business RV Series VPN routers

TA202128

Threat Level Amber

Publish Date – Aug 5, 2021

Cisco has patched serious vulnerabilities that might be exploited by sending maliciously crafted HTTP requests to the web-based management interfaces of vulnerable Small Business RV Series Routers. However, the remote management feature is disabled by default on all impacted VPN routers. The threat research team at Hive Pro hasn't observed any exploits of these flaws in the wild, yet it is strongly recommended to patch the reported vulnerabilities.

Vulnerability Details

CVE ID	Affected Products	Affected CPEs	Vulnerability Name	CWE ID
CVE-2021-1609	Cisco VPN Router RV340, RV340W ,RV345, RV345P	cpe:2.3:h:cisco:rv340:*:*:*:*:*:*:*:*,cpe:2.3:h:cisco:rv340w:*:*:*:*:*:*:*:*, cpe:2.3:h:cisco:rv345:*:*:*:*:*:*:*:*, cpe:2.3:h:cisco:rv345p:*:*:*:*:*:*:*:*	Web Management Remote Code Execution and Denial of Service Vulnerability	CWE-121
CVE-2021-1610			Web Management Command Injection Vulnerability	CWE-149
CVE-2021-1602	Cisco VPN Router RV160,RV160W,RV260, RV260P,RV260W	cpe:2.3:h:cisco:rv160:*:*:*:*:*:*:*:* , cpe:2.3:h:cisco:rv160w:*:*:*:*:*:*:*:* , cpe:2.3:h:cisco:rv260:*:*:*:*:*:*:*:* , cpe:2.3:h:cisco:rv260p:*:*:*:*:*:*:*:* , cpe:2.3:h:cisco:rv260w:*:*:*:*:*:*:*:*	Remote Command Execution Vulnerability	CWE-78

Patch Link

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv340-cmdinj-rcedos-pY8J3qfy
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-code-execution-9UVJr7k4

References

https://thehackernews.com/2021/08/cisco-issues-critical-security-patches.html
https://www.bleepingcomputer.com/news/security/cisco-fixes-critical-high-severity-pre-auth-flaws-in-vpn-routers/