UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00181

CRITICAL CISCO VPN BUGS

DATE ISSUED: 9th August 2021

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

Approximately 8,800 systems are open to exploitation using a slew of critical bugs and vulnerabilities affecting various models that could allow an attacker to remotely take over the machine and run arbitrary code.

BREAKDOWN

By default, remote management of these services is disabled however, Internet scans have determined numerous devices are publicly accessible.

Systems affected and vulnerabilities include:

- Cisco RV340, RV340W, RV345, RV345P Dual WAN Gigabit VPN Routers Web Management Vulnerabilities
- Cisco Small Business RV160 and 260 series VPN Routers Remote Command Executions Vulnerability
- Cisco Packet Tracer for Windows DLL Injection Vulnerability
- Cisco Network Services Orchestrator CLI Secure Shell Server Privilege Escalation Vulnerability
- ConfD CLI Secure Shell Server Privilege Escalation Vulnerability.

REMEDIATION STEPS

- Older routers no longer under support must be upgraded to newer models as they will not have patches available (including RV1100W, RV130, RV130W & RV215W reached EOL 2018).
- See advisories below for advice and information from Cisco and apply available patches.

REFERENCES & RESOURCES

Threatpost	https://threatpost.com/critical-cisco-bug-vpn-routers/168449/
ZDNet	https://www.zdnet.com/article/cisco-says-it-wont-patch-74-security-bugs-in-older-rv-routers-that-reached-eol/
Cisco Bug Tool	https://www.cisco.com/c/en/us/support/web/tools/bst/bsthelp/index.html
Cisco	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv340-cmdinj-rcedos-pY8J3qfy
	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-packettracer-dll-inj-Qv8Mk5Jx
	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nso-priv-esc-XXqRtTfT
	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-code-execution-9UVJr7k4
	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-confd-priv-esc-LsGtCRx4