National Cyber Security Centre

2208041241-NCSC

A part of the **Department of the Environment, Climate & Communications**

NCSC Alert

Cisco Small Business RV Series Routers Vulnerabilities
05 August 2022

Status: TLP-CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP-CLEAR *when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules,* TLP-CLEAR *information may be shared without restriction.* For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

Description

Cisco have released an advisory in relation to multiple vulnerabilities in Cisco Small Business RV160, RV260, RV340, and RV345 Series Routers that could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device.
NOTE: There are no workarounds that address these vulnerabilities.

CVE(s)

CVE-2022-20827 (CVSS Base Score: 9.0), CVE-2022-20841 (CVSS Base Score: 8.3),CVE-2022-20842 (CVSS Base Score: 9.8)

Products Affected

CVE-2022-20827 and CVE-2022-20841 affect the following Cisco products:

- RV160 VPN Routers
- RV160W Wireless-AC VPN Routers
- RV60 VPN Routers
- RV260P VPN Routers with PoE
- RV260W Wireless-AC VPN Routers
- RV340 Dual WAN Gigabit VPN Routers
- RV340W Dual WAN Gigabit Wireless-AC VPN Routers
- RV345 Dual WAN Gigabit VPN Routers
- RV345P Dual WAN Gigabit POE VPN Routers

CVE-2022-20842 affects the following Cisco products:

- RV340 Dual WAN Gigabit VPN Routers
- RV340W Dual WAN Gigabit Wireless-AC VPN Routers
- RV345 Dual WAN Gigabit VPN Routers
- RV345P Dual WAN Gigabit POE VPN Routers

Impact

Remote Code Execution - compromised systems, data loss.

Recommendations

The NCSC recommends that affected organisations review the Cisco advisory here. Cisco has released free software updates that address these vulnerabilities - customers with service contracts that entitle them to regular software updates should obtain security fixes through their usual update channels.

DISCLAIMER: *This document is provided "as is" without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.*

National Cyber Security Centre
29-31 Adelaide Road,
Dublin, D02 X285,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@decc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie
LinkedIn: ncsc-ie