Computer Emergency Response Team

BOLLETTINO IT-CERT.190228.B01

Vulnerabilità critica in dispositivi Cisco RV110W, RV130W e RV215W (CVE-2019-1663)

MINISTERO DELLO
SVILUPPO ECONOMICO

DESCRIZIONE

È stata scoperta una vulnerabilità critica (CVE-2019-1663) nell'interfaccia Web di gestione dei prodotti **Cisco RV110W Wireless-N VPN Firewall**, **Cisco RV130W Wireless-N Multifunction VPN Router** e **Cisco RV215W Wireless-N VPN Router**.

La vulnerabilità è legata ad una validazione impropria dei dati forniti dall'utente all'interfaccia di gestione basata sul Web di questi dispositivi. Questa interfaccia è accessibile sia da una LAN locale, sia attraverso la funzionalità di gestione remota (disabilitata per impostazione predefinita).

Un attaccante potrebbe sfruttare questa vulnerabilità inviando ad un dispositivo affetto richieste HTML appositamente predisposte. Se sfruttata con successo, questa vulnerabilità potrebbe consentire l'esecuzione di codice arbitrario da remoto con privilegi elevati sul sistema operativo sottostante.

Al momento non ci sono notizie che questa vulnerabilità sia stata sfruttata in attacchi reali.

Cisco ha rilasciato aggiornamenti software che risolvono la vulnerabilità nei prodotti interessati. Non sono disponibili soluzioni alternative per mitigare questa vulnerabilità (per maggiori informazioni si veda la sezione LINK UTILI).

SOLUZIONE

Cisco ha rilasciato aggiornamenti software che risolvono la vulnerabilità descritta in questo bollettino.

I gestori di dispositivi Cisco RV110W, RV130W e RV215W devono installare gli aggiornamenti relativi alla propria piattaforma, dopo appropriato *testing*.

Per maggiori informazioni sui prodotti vulnerabili e sugli aggiornamenti disponibili, si raccomanda di consultare il relativo bollettino di sicurezza di Cisco (si veda la sezione LINK UTILI).

SISTEMI

Risultano affetti dalla vulnerabilità descritta in questo bollettino i seguenti apparati Cisco:

- RV110W Wireless-N VPN Firewall: *release* precedenti la 1.2.2.1
- RV130W Wireless-N Multifunction VPN Router: *release* precedenti la 1.0.3.45
- RV215W Wireless-N VPN Router: *release* precedenti la 1.3.1.1

LINK UTILI

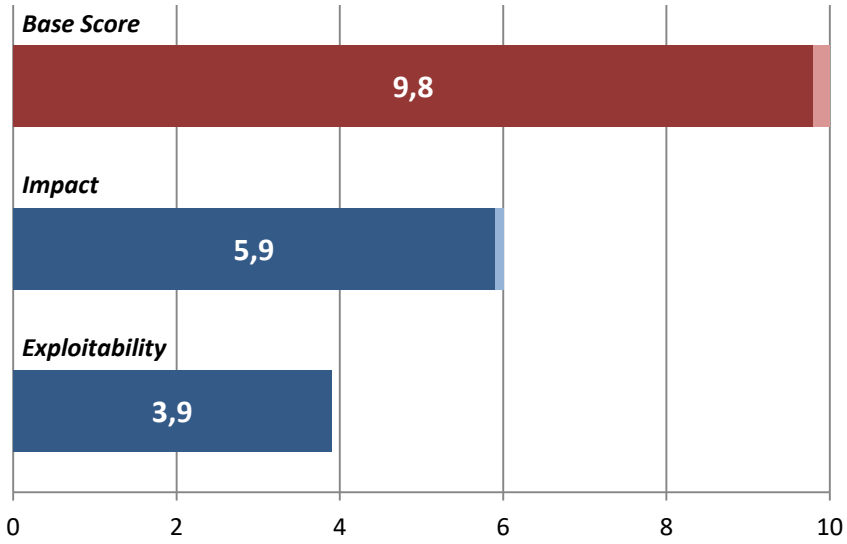
Avviso del produttore

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190227-rmi-cmd-ex

Mitre CVE ID

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1663

VALUTAZIONE CVSS



Relativamente alla valutazione della *severity* come metrica di base - da intendersi quale livello di pericolosità della vulnerabilità delle componenti di sistema o delle piattaforme - il CERT Nazionale valuta i parametri che concorrono al calcolo della *Base Score* secondo lo standard CVSS v3 (*Common Vulnerabilities Scoring System*), avvalendosi del *tool* messo a disposizione dal sito del NIST (https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator).

Nello specifico sono stati raggiunti i seguenti punteggi:

- *Base Score:* 9,8
- *Impact:* 5,9
- *Exploitability:* 3,9

Vettore CVSS: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

NOTE

Le informazioni contenute nel presente bollettino sono fornite a meri fini informativi.

In nessun caso il CERT Nazionale può essere ritenuto responsabile di qualunque perdita, pregiudizio, responsabilità, costo, onere o spesa, ivi comprese le eventuali spese legali, danno diretto, indiretto, incidentale o consequenziale, derivante da o connesso alle informazioni riportate nel presente bollettino.

La versione PDF del bollettino è statica ed, in quanto tale, contiene le informazioni disponibili al momento della pubblicazione.