Hive Pro

THREAT ADVISORY

Cisco patched multiple critical vulnerabilities in StarOS Software

TA2022015

Threat Level AMBER

Publish Date – Jan 20, 2022

Cisco patched two critical vulnerabilities in Redundancy Configuration Manager for StarOS software. Exploitation of one of the vulnerabilities is not required to exploit the other vulnerability.

An attacker could exploit the remote code execution vulnerability (CVE-2022-20649) by connecting to the device and navigating to the service with debug mode enabled. This vulnerability in Cisco RCM for Cisco StarOS Software could allow an unauthenticated attacker to perform remote code execution on the application with *root*-level privileges in the context of the configured container.

The second vulnerability (CVE-2022-20648) is an Information Disclosure Vulnerability that exists because of a debug service that incorrectly listens to and accepts incoming connections. An attacker could exploit this vulnerability by connecting to the debug port and executing debug commands. A successful exploit could result in the disclosure of confidential information that should be restricted.

HivePro threat researchers advise customers to patch the vulnerabilities using the link given below.

Vulnerability Details

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2022-20649	Cisco RCM for StarOS Earlier than 21.25	cpe:2.3:o:cisco:staros:*:*:*:*:*:*:*:*	Cisco RCM Debug Remote Code Execution Vulnerability	CWE-264
CVE-2022-20648			Cisco RCM Debug Information Disclosure Vulnerability	CWE-200

Patch Link

https://tools.cisco.com/security/center/resources/security_vulnerability_policy.html#ssu

References

Cisco advisory
https://www.cisa.gov/uscert/ncas/current-activity/2022/01/20/cisco-releases-security-updates-multiple-products
https://threatpost.com/critical-cisco-staros-bug-root-access-debug-mode/177832/