Advisory Alert

Alert Number: **AAA20220513** **Date:** **May 13, 2022**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
SonicWall	**High**	Multiple Vulnerabilities
Cisco	**High**	Multiple Vulnerabilities

Description

Affected Product	**SonicWall**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-22282)
Description	SonicWall has released a security update addressing Multiple Vulnerabilities that exists in SonicWall SSLVPN SMA1000 series appliances. An attacker could exploit these vulnerabilities to trigger an Unauthenticated access control bypass, Use of a shared and hard-coded encryption key, and Open redirection on the targeted appliances. SonicWall highly recommends applying necessary fixes immediately to avoid issues.
Affected Products	SMA 1000 Series - SMA 6200, 6210, 7200, 7210, 8000v (ESX, KVM, Hyper-V, AWS, Azure)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0009

Affected Product	**Cisco**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-20681, CVE-2022-20677, CVE-2022-20718, CVE-2022-20719, CVE-2022-20720, CVE-2022-20721, CVE-2022-20722, CVE-2022-20723, CVE-2022-20724, CVE-2022-20725, CVE-2022-20726, CVE-2022-20727)
Description	Cisco has released Security Updates addressing multiple vulnerabilities that exist with various cisco products such as Parameter Injection, Path Traversal, Arbitrary Code Execution, Cross-Site Scripting, User Impersonation, Denial of Service, Privilege Escalation and Arbitrary File Read Vulnerability. Cisco highly recommends applying necessary fixes immediately to avoid issues.
Affected Products	800 Series Industrial Integrated Services Routers (Industrial ISRs) 800 Series Integrated Services Routers (ISRs) 1000 Series Connected Grid Router (CGR1000) Compute Modules IC3000 Industrial Compute Gateways Industrial Ethernet (IE) 4000 Series Switches IOS XE-based devices configured with IOx IR510 WPAN Industrial Routers Cisco Catalyst 9000 Family Switches Cisco Catalyst 9000 Family Wireless Controllers
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ewlc-priv-esc-ybvHKO5 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-yuXQ6hFj

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.