TLP: WHITE

Advisory Alert

Alert Number : AAA20220428 **Date :** April 28, 2022

Document Classification Level : Public Circulation Permitted

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Redhat	**High**	Stack Overflow Vulnerability
Sonicwall	**High, Medium**	Multiple Vulnerabilities
Cisco	**High**	Multiple Vulnerabilities

Description

Affected Product	Redhat
Severity	**High**
Affected Vulnerability	Stack Overflow Vulnerability (CVE-2022-0435)
Description	Redhat has released Security Updates addressing a stack overflow flaw vulnerability found in the Linux kernel's TIPC protocol functionality which leads a remote user to cause system crash and Privilege Escalation.
Affected Products	Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.1 ppc64le Red Hat Enterprise Linux Server for x86_64 - Update Services for SAP Solutions 8.1 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2022:1619

Affected Product	SonicWall
Severity	**High, Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-22275, CVE-2022-22276, CVE-2022-22277, CVE-2022-22278, CVE-2021-20051)
Description	Sonicwall has release Security updates for multiple vulnerabilities for SonicOS and SonicWall Global VPN Client. **CVE-2022-22275** - Improper Restriction of TCP Communication Channel in HTTP/S inbound traffic from WAN to DMZ bypassing security policy until TCP handshake potentially causing Denial of Service attack if a target host is vulnerable. **CVE-2022-22276** - A vulnerability that existing SonicOS SNMP service could cause exposure of sensitive information to an unauthorized user **CVE-2022-22277** - A vulnerability that existing SonicOS SNMP service could cause exposure of Wireless Access Point sensitive information in cleartext. **CVE-2022-22278** - A vulnerability that existing SonicOS CFS returns a large 403 forbidden HTTP response message to the source address when a user tries to access a prohibited resource which allows an attacker to cause HTTP Denial of Service (DoS) attack **CVE-2021-20051** - A successful exploitation of DLL Search Order Hijacking vulnerability which exist in one of the installer components of SonicWall Global VPN Client installer could result in command execution in the target system.
Affected Products	SonicOS Gen7 TZ Series 7.0.1-5030-R2007 and earlier versions SonicOS Gen7 NSa Series 7.0.1-5030-R2007 and earlier versions SonicOS Gen7 NSv Series 7.0.1.0-5030-1391 and earlier versions SonicOS Gen7 NSsp Series 7.0.1-5030-R780 and earlier versions SonicOS Gen6 TZ Series 6.5.4.9-93n and earlier versions SonicOS Gen6 NSa Series 6.5.4.9-93n and earlier versions Global VPN Client 4.10.7.1424 (32-bit & 64-bit)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0004 https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0036

Affected Product	Cisco
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-20746,CVE-2022-20751, CVE-2022-20757,CVE-2022-20743,CVE-2022-20759,CVE-2022-20742,CVE-2022-20760,CVE-2022-20745,CVE-2022-20737,CVE-2022-20715,CVE-2022-20767,CVE-2022-20681,CVE-2022-20729,CVE-2022-20730,CVE-2022-20748,CVE-2022-20627,CVE-2022-20628,CVE-2022-2062,CVE-2022-20740,CVE-2022-20744)
Description	Cisco has released security updates addressed multiple vulnerabilities that exists in multiple products. Which may lead attackers to cause denial of service attacks, privilege escalation vulnerability, Cross-site Scripting, XML injection and Information Disclosure vulnerability. Cisco highly recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/publicationListing.x?product=Cisco&key-word=2022%20Apr%2027&last_published=2022%20Apr&sort=-day_sir#~Vulnerabilities

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.