Advisory Alert

Alert Number: AAA20210924 **Date:** September 24, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Sonicwall	Critical	Multiple Vulnerabilities
NetGear	Critical	Remote Code Execution
Redhat	High	Multiple Vulnerabilities

Description

Affected Product	**SonicWall**
Severity	**Critical**
Affected Vulnerability	**Multiple Vulnerabilities** (CVE-2021-20034, CVE-2021-20037)
Description	CVE-2021-20034: An improper access control vulnerability in **SMA100** allows a remote unauthenticated attacker to bypass the path traversal checks and delete an arbitrary file potentially resulting in a reboot to factory default settings. CVE-2021-20037: SonicWall Global VPN Client installer incorrect default file permission vulnerability leads to privilege escalation which potentially allows command execution in the host operating system.
Affected Products	9.0.0.10-28sv and earlier 10.2.0.7-34sv and earlier 10.2.1.0-17sv and earlier Global VPN Client 4.10.5 and earlier
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.sonicwall.com/support/product-notification/security-notice-critical-arbitrary-file-delete-vulnerability-in-sonicwall-sma-100-series-appliances/210819124854603/ https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0024

Affected Product	**Netgear**
Severity	**Critical**
Affected Vulnerability	**Remote Code Execution (**CVE-2021-40847)
Description	The flaw in Netgear routers could be exploited by a remote attacker to execute arbitrary code as root via man in the middle attack. Netgear highly recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	R6400v2 R6700 R6700v3 R6900 R6900P R7000 R7000P R7850 R7900 R8000 RS400
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://kb.netgear.com/000064039/Security-Advisory-for-Remote-Code-Execution-on-Some-Routers-PSV-2021-0204

Affected Product	**Redhat**
Severity	**High**
Affected Vulnerability	**Multiple Vulnerabilities** (CVE-2020-13936, CVE-2021-3536, CVE-2021-3597, CVE-2021-3642, CVE-2021-3644, CVE-2021-3690, CVE-2021-21295, CVE-2021-21409, CVE-2021-28170, CVE-2021-29425)
Description	Redhat has released Security Updates addressing multiple vulnerabilities that exists with JBoss Enterprise Application Platform. Redhat highly recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	JBoss Enterprise Application Platform 7.4 for RHEL 7 x86_64 JBoss Enterprise Application Platform 7.4 for RHEL 8 x86_64 JBoss Enterprise Application Platform Text-Only Advisories x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2021:3656 https://access.redhat.com/errata/RHSA-2021:3658 https://access.redhat.com/errata/RHSA-2021:3660

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.