Advisory Alert

Alert Number: AAA20220722 **Date:** July 22, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
SonicWall	**Critical**	Unauthenticated SQL Injection Vulnerability
RedHat	**High**	Multiple vulnerabilities

Description

Affected Product	**SonicWall**
Severity	**Critical**
Affected Vulnerability	Unauthenticated SQL Injection Vulnerability (CVE-2022-22280)
Description	SonicWall has released a patch update addressing an Unauthenticated SQL Injection vulnerability that exists in their SonicWall GMS and Analytics On-Prem products. This vulnerability exists because of Improper Neutralization of Special Elements used in the SQL Commands. SonicWall highly recommended to apply necessary fixes at earliest to avoid issues
Affected Products	SonicWall GMS 9.3.1-SP2-Hotfix1 and earlier versions SonicWall Analytics On-Prem 2.5.0.3-2520 and earlier versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0007

Affected Product	**RedHat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-27666, CVE-2022-28733)
Description	RedHat has released a patch update addressing multiple vulnerabilities that exist in the imgbased, redhat-release-virtualization-host, and redhat-virtualization-host that is used in the Red Hat Virtualization 4 for Red Hat Enterprise Linux 8. **CVE-2022-27666** - Kernel: buffer overflow in IPsec ESP transformation code **CVE-2022-28733** - Grub2: Integer underflow in grub_net_recv_ip4_packets RedHat highly recommends to apply necessary security fixes at earliest to avoid issues
Affected Products	Red Hat Virtualization 4 for RHEL 8 x86_64 Red Hat Virtualization Host 4 for RHEL 8 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2022:5678

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.