Advisory Alert

Alert Number : AAA20210421 **Date :** April 21, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
SonicWall	**Critical**	**Zero-Day Vulnerabilities**
Oracle	**Critical**	**Multiple Vulnerabilities**
IBM	**High**	**XML External Entity (XXE)**

Description

Affected Product	**SonicWall**
Severity	**Critical**
Affected Vulnerability	Zero-Day Vulnerabilities (CVE-2021-20021, CVE-2021-20022, CVE-2021-20023)
Description	SonicWall has addressed a zero day vulnerabilities in the SonicWall Email Security. These vulnerabilities were executed in conjunction to obtain following attacks, **CVE-2021-20021 -** an administrative account by sending a crafted HTTP request to the remote host. **CVE-2021-20022 -** post authenticated attacker to upload an arbitrary file to the remote host **CVE-2021-20023 -** post authenticated attacker to read an arbitrary file on the remote host. SonicWall advise active support license and upgrade to the latest SonicWall Email Security version.
Affected Products	SonicWall On-premise Email Security 10.0.9 and earlier versions Hosted Email Security 10.0.9 and earlier versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0007 https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0008 https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0010 https://www.sonicwall.com/support/product-notification/security-notice-sonicwall-email-security-zero-day-vulnerabilities/210416112932360/

Affected Product	**Oracle**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Oracle has released its April 2021 security patch update which address multiple vulnerabilities across several of products. Which an attacker could use to gain control of an affected systems. Oracle highly recommends to apply relevant patches at earliest to avoid issues.
Affected Products	Multiple products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.oracle.com/security-alerts/cpuapr2021.html

Affected Product	**IBM**
Severity	**High**
Affected Vulnerability	XML External Entity (XXE) (CVE-2021-20454)
Description	IBM Web Sphere Application Server is vulnerable to XML External Entity Injection attack when processing XML data. A remote attacker could exploit this vulnerability ability to expose sensitive data or consume memory resources.
Affected Products	WebSphere Application Server 7.0 WebSphere Application Server 8.0 WebSphere Application Server 8.5 WebSphere Application Server 9.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6445481

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.