Advisory Alert

Alert Number: AAA20221102 **Date:** November 2, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
OpenSSL	**High**	Multiple OpenSSL Vulnerabilities
RedHat	**High**	
Juniper	**High**	
IBM	**High**	
FortiGate	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Redhat	**High**	Multiple Vulnerabilities
Citrix	**Medium**	Multiple Vulnerabilities
Ubuntu	**Medium**	System Crash Vulnerability
Apache	**Low**	Request Smuggling Vulnerability

Description

Affected Product	**OpenSSL , Redhat, Juniper, IBM**
Severity	**High**
Affected Vulnerability	Multiple OpenSSL Vulnerabilities (CVE-2022-3786, CVE-2022-3602)
Description	OpenSSL has released Security Updates addressing multiple vulnerabilities. Patch updates are available for Red Hat Linux, Juniper and IBM products that uses this vulnerable version of the OpenSSL. **CVE-2022-3786** - A Denial of service (DoS) attack is possible due to the vulnerability. A boundary mistake occurred when an X.509 certificate was processing the email address field length, which led to the vulnerability. A remote attacker can supply a specially crafted certificate to the application, trigger a buffer overflow and crash the application. **CVE-2022-3602** - The vulnerability allows a remote attacker to execute arbitrary code on the target system. The email address field inside the X.509 certificate was processed with a boundary error, which results in the vulnerability. A remote attacker can supply a specially crafted certificate to the application, trigger a 4-byte buffer overflow and execute arbitrary code on the target system.
Affected Products	**OpenSSL** OpenSSL versions 3.0.0 to 3.0.6 are vulnerable to this issue **Redhat** Red Hat Enterprise Linux for x86_64 9 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.0 x86_64 Red Hat Enterprise Linux for IBM z Systems 9 s390x Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.0 s390x Red Hat Enterprise Linux for Power, little endian 9 ppc64le Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.0 ppc64le Red Hat Enterprise Linux for ARM 64 9 aarch64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.0 aarch64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.0 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.0 x86_64 Red Hat Enterprise Linux Server for ARM 64 - 4 years of updates 9.0 aarch64 Red Hat Enterprise Linux Server for IBM z Systems - 4 years of updates 9.0 s390x **Juniper** Juniper Networks Junos OS Evolved versions later than 22.1R1-EVO. **IBM** Storage Node machine 9840-AE1, 9843-AE1, 9840-AE2, 9843-AE2, 9840-AE3, 9843-AE3, and 9843-UF3 Storage node code versions VRMFs prior to 1.5.2.12, VRMFs prior to 1.6.1.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	**OpenSSL** https://www.openssl.org/news/secadv/20221101.txt **Redhat** https://access.redhat.com/errata/RHSA-2022:7288 **Juniper** https://supportportal.juniper.net/s/article/2022-11-Out-of-Cycle-Security-Bulletin-High-severity-security-issues-resolved-in-OpenSSL-3-0-7-CVE-2022-3602-CVE-2022-3786?language=en_US **IBM** https://www.ibm.com/support/pages/node/6832966 https://www.ibm.com/support/pages/node/6622017

Affected Product	**FortiGate**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-26122, CVE-2022-38374, CVE-2022-35851, CVE-2022-38381, CVE-2022-33878, CVE-2022-38373, CVE-2022-39949, CVE-2022-39945, CVE-2022-39950, CVE-2022-30307, CVE-2022-38380, CVE-2022-35842, CVE-2022-26119, CVE-2022-38372, CVE-2022-33870, CVE-2022-42473)
Description	Fortinet has released Security Updates addressing multiple vulnerabilities that exist with fortinet products. These vulnerabilities allow Privilege Escalation, SQL Injection, Information Disclosure, Improper Access Control, and XSS on the affected systems. It is highly recommended to apply the necessary fixes provided on the official Fortinet website at the earliest to avoid these security issues.
Affected Products	FortiOS/FortiMail/FortiClient running AV engine version 6.4.274, 6.2.168 and below. FortiADC version 5.0.0, 5.1.0, 5.2.0, 5.3.0, 5.4.0, 6.0.0, 6.1.0, 6.2.0, 7.0.0, 7.1.0 FortiClientMac version 7.0.0 through 7.0.5 FortiDeceptor version 4.2.0 FortiDeceptor version 4.1.0 through 4.1.1 FortiDeceptor version 4.0.2 FortiEDR CollectorWindows version 4.0.0, 5.0.0, 5.1.0 FortiMail version 6.0.0, 6.2.0, 6.4.0, 7.0.0, 7.2.0, , FortiAnalyzer 6.2 all versions 6.4.0, 7.0.0 through 7.0.4 FortiOS version 6.4.0, 6.4.9, 7.0.0,7.2.0, 7.0.6 FortiSIEM version 5.0.0, 5.2.1, 5.2.5, 5.3.0, 5.4.0, 6.2.0, 6.3.0, 6.4.0 through 6.4.1 FortiTester version 2.3.0, 2.4.0, 2.5.0, 2.6.0, 2.7.0, 2.8.0, 2.9.0, 3.0.0, 3.1.0, 3.2.0, 3.3.0, 3.4.0, 3.5.0, 3.6.0, 3.7.0, 3.8.0, 3.9.0, 4.1.0, 4.2.0, 7.0.0,7.1.0, 7.2.0 FortiSOAR version 7.0.0 through 7.0.3 FortiSOAR version 6.4.0 through 6.4.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-22-074 https://www.fortiguard.com/psirt/FG-IR-22-232 https://www.fortiguard.com/psirt/FG-IR-22-314 https://www.fortiguard.com/psirt/FG-IR-22-234 https://www.fortiguard.com/psirt/FG-IR-22-246 https://www.fortiguard.com/psirt/FG-IR-22-331 https://www.fortiguard.com/psirt/FG-IR-22-218 https://www.fortiguard.com/psirt/FG-IR-22-066 https://www.fortiguard.com/psirt/FG-IR-21-228 https://www.fortiguard.com/psirt/FG-IR-22-228 https://www.fortiguard.com/psirt/FG-IR-22-174 https://www.fortiguard.com/psirt/FG-IR-22-223 https://www.fortiguard.com/psirt/FG-IR-22-064 https://www.fortiguard.com/psirt/FG-IR-22-216 https://www.fortiguard.com/psirt/FG-IR-22-070 https://www.fortiguard.com/psirt/FG-IR-22-283

Affected Product	**Redhat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-3515, CVE-2022-2588, CVE-2022-21123, CVE-2022-21125, CVE-2022-21166)
Description	Redhat has released security updates addressing multiple vulnerabilities that exist in their products. Attackers can exploit these vulnerabilities to cause remote code execution and privilege escalation. Redhat recommends to apply necessary security fixes at earliest to avoid issues
Affected Products	Red Hat Enterprise Linux Server - AUS 8.2 x86_64 Red Hat Enterprise Linux Server - TUS 8.2 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.2 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.2 x86_64 Red Hat Enterprise Linux for Real Time - Telecommunications Update Service 8.2 x86_64 Red Hat Enterprise Linux for Real Time for NFV - Telecommunications Update Service 8.2 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2022:7283 https://access.redhat.com/errata/RHSA-2022:7280 https://access.redhat.com/errata/RHSA-2022:7279

Affected Product	**Citrix**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-42316, CVE-2022-42317, CVE-2022-42318, CVE-2022-42323)
Description	Citrix has released Security Updates addressing multiple Vulnerabilities that exist in their products. Which may allow a privileged user in a guest VM to cause part of the management service to become unresponsive, resulting in the inability to create new guests or modify the configuration of running guests. Citrix recommends to apply necessary security fixes at earliest to avoid issues
Affected Products	Citrix Hypervisor 8.2 LTSR CU1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.citrix.com/article/CTX472851/citrix-hypervisor-security-bulletin-for-cve202242316-cve202242317-cve202242318

Affected Product	**Ubuntu**
Severity	**Medium**
Affected Vulnerability	System Crash Vulnerability (CVE-2021-46848)
Description	Ubuntu has released a security updates to address a vulnerability that could leads to system crash in the libtasn 1-6 package. This vulnerability exists due to Libtasn1 did not properly perform bounds checking. An attacker could possibly use this issue to cause a crash. Ubuntu recommends to apply necessary security fixes at earliest to avoid issues
Affected Products	GNU Libtasn1 before 4.19.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-5707-1

Affected Product	**Apache**
Severity	**Low**
Affected Vulnerability	Request Smuggling vulnerability (CVE-2022-42252)
Description	Apache has released Security Updates addressing a request smuggling vulnerability that exist in their products. This vulnerability exists due to incorrect HTTP request validation. A remote attacker has the ability to smuggle arbitrary HTTP headers via an incorrect Content-Length header and send the server a specially crafted HTTP request. If the vulnerability is successfully exploited, an attacker may be able to compromise HTTP cache and launch phishing attacks, however Tomcat must be set up to ignore incorrect HTTP headers by setting rejectIllegalHeader to false. Apache recommends to apply necessary security fixes at earliest to avoid issues
Affected Products	Apache Tomcat 10.1.0-M1 to 10.1.0 Apache Tomcat 10.0.0-M1 to 10.0.26 Apache Tomcat 9.0.0-M1 to 9.0.67 Apache Tomcat 8.5.0 to 8.5.52
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tomcat.apache.org/security-10.html https://tomcat.apache.org/security-9.html https://tomcat.apache.org/security-8.html

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.