Advisory Alert

Alert Number: AAA20230308 **Date:** March 8, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
FortiGuard	**Critical**	Buffer Underflow Vulnerability
Redhat	**High**	Multiple Vulnerabilities
Apache	**High**	HTTP Response Smuggling vulnerability
Veeam	**High**	Sensitive Information Disclosure vulnerability
Ubuntu	**High** , **Medium**, **Low**	Multiple Vulnerabilities
FortiGuard	**High** , **Medium**, **Low**	Multiple Vulnerabilities
IBM	**Medium**	Denial of service vulnerability

Description

Affected Product	**FortiGuard**
Severity	**Critical**
Affected Vulnerability	Buffer Underflow Vulnerability (CVE-2023-25610)
Description	FortiGuard has released a Security Update addressing a Heap Buffer Underflow Vulnerability that exist in FortiOS & FortiProxy administrative interface. Using this vulnerability a remote unauthenticated attacker can execute arbitrary code on the device and/or perform a DoS on the GUI, via specifically crafted requests. FortiGuard highly recommends to apply necessary security fixes at earliest to avoid issues
Affected Products	FortiOS version 7.2.0 through 7.2.3 FortiOS version 7.0.0 through 7.0.9 FortiOS version 6.4.0 through 6.4.11 FortiOS version 6.2.0 through 6.2.12 FortiOS 6.0 all versions FortiProxy version 7.2.0 through 7.2.2 FortiProxy version 7.0.0 through 7.0.8 FortiProxy version 2.0.0 through 2.0.11 FortiProxy 1.2 all versions FortiProxy 1.1 all versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-23-001

Affected Product	**Redhat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-4378, CVE-2022-42703)
Description	Redhat has released Security Updates addressing multiple vulnerabilities that exist in their products. Attackers can exploit these vulnerabilities to cause stack overflow and create use-after-free condition. **CVE-2022-4378**- Stack overflow vulnerability in do_proc_dointvec and proc_skip_spaces functions. A local user can trigger a stack-based buffer overflow and execute arbitrary code with elevated privileges. **CVE-2022-42703**- use-after-free vulnerability exists due to a use-after-free error within the Linux kernel, related to leaf anon_vma double reuse. A local user can trigger a use-after-free error and crash the kernel. Redhat recommends to apply necessary security fixes at earliest to avoid issues
Affected Products	Red Hat Enterprise Linux Desktop 7 x86_64 Red Hat Enterprise Linux for IBM z Systems 7 s390x Red Hat Enterprise Linux for Power, big endian 7 ppc64 Red Hat Enterprise Linux for Power, little endian 7 ppc64le 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 Red Hat Enterprise Linux for Scientific Computing 7 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.2 x86_64 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 7 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.2 ppc64le Red Hat Enterprise Linux Workstation 7 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2023:1110 https://access.redhat.com/errata/RHSA-2023:1109 https://access.redhat.com/errata/RHSA-2023:1103 https://access.redhat.com/errata/RHSA-2023:1101 https://access.redhat.com/errata/RHSA-2023:1091

Affected Product	**Apache**
Severity	**High**
Affected Vulnerability	HTTP Response Smuggling vulnerability (CVE-2023-25690, CVE-2023-27522)
Description	Apache has released security updates to address multiple HTTP Response Smuggling vulnerabilities that exists in their products. These vulnerabilities allows an attacker to compromise vulnerable systems. **CVE-2023-25690**- The vulnerability exists due to software does not correclty process CRLF character sequences in mod_rewrite and mod_proxy. A remote attacker can send specially crafted request containing CRLF sequence and make the application to send a split HTTP response **CVE-2023-27522**- The vulnerability exists due to software does not correclty process CRLF character sequences in mod_proxy_uwsgi. A remote attacker can send specially crafted request containing CRLF sequence and make the application to send a split HTTP response. Apache recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Apache HTTP Server: 2.4.32 - 2.4.55
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://httpd.apache.org/security/vulnerabilities_24.html

Affected Product	**Veeam**
Severity	**High**
Affected Vulnerability	Sensitive Information Disclosure vulnerability (CVE-2023-27532)
Description	Veeam has released a security update to address Sensitive Information Disclosure vulnerability that exists in their Backup & Replication component. Veeam.Backup.Service.exe allows an unauthenticated user to request encrypted credentials stored in the configuration database which may lead to gaining access to the backup infrastructure hosts. Veeam recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Veeam Backup & Replication version between 9.5 U4b (9.5.4.2866) and 11 (11.0.0.837 P20210525) Veeam Backup & Replication version between 10a (10.0.1.4854) and 11a (11.0.1.1261 P20230227)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.veeam.com/kb4424

Affected Product	**Ubuntu**
Severity	**High** , **Medium** , **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-3669, CVE-2022-3169, CVE-2022-3344, CVE-2022-3424, CVE-2022-3435, CVE-2022-3521, CVE-2022-3545, CVE-2022-3623, CVE-2022-3628, CVE-2022-36280, CVE-2022-3640, CVE-2022-41218, CVE-2022-4139, CVE-2022-42328, CVE-2022-42329, CVE-2022-42895, CVE-2022-42896, CVE-2022-4378, CVE-2022-4379, CVE-2022-43945, CVE-2022-45869, CVE-2022-47518, CVE-2022-47519, CVE-2022-47520, CVE-2022-47521, CVE-2022-47929, CVE-2023-0045, CVE-2023-0179, CVE-2023-0266, CVE-2023-0394, CVE-2023-0461, CVE-2023-0468, CVE-2023-20938, CVE-2023-23454, CVE-2023-23455, CVE-2023-23559)
Description	Ubuntu has released security updates to address multiple vulnerabilities that exists in their products. These vulnerabilities allows an attacker to cause use-after-free, out-of-bounds, denial of service and integer overflow Ubuntu recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Ubuntu 16.04 Ubuntu 18.04 Ubuntu 20.04 Ubuntu 22.04 Ubuntu 22.10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-5927-1 https://ubuntu.com/security/notices/USN-5929-1 https://ubuntu.com/security/notices/LSN-0092-1 https://ubuntu.com/security/notices/USN-5934-1 https://ubuntu.com/security/notices/USN-5935-1

Affected Product	**FortiGuard**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-25611, CVE-2023-23776, CVE-2022-29056, CVE-2022-27490, CVE-2022-40676, CVE-2022-39953, CVE-2022-45861, CVE-2022-41328, CVE-2022-42476, CVE-2022-41329, CVE-2022-41333, CVE-2023-25605, CVE-2022-39951, CVE-2022-22297)
Description	FortiGuard has released Security Updates addressing multiple vulnerabilities that exist in their products. Successful exploitation of these vulnerabilities could lead to unauthorized code or command execution, information disclosure, improper access control and denial of service. FortiGuard recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	FortiAnalyzer version 7.2.0 through 7.2.1 FortiAnalyzer version 7.0.0 through 7.0.5 FortiAnalyzer 6.4 all versions FortiAnalyzer version 7.0.0 through 7.0.4 FortiAnalyzer version 6.4.0 through 6.4.10 FortiAuthenticator version 6.4 all versions FortiAuthenticator version 6.3 all versions FortiAuthenticator version 6.2 all versions FortiAuthenticator version 6.1 all versions FortiAuthenticator version 6.0 all versions FortiAuthenticator version 5.5 all versions FortiAuthenticator version 5.4 all versions FortiDeceptor version 3.1 , 3.0 all versions FortiDeceptor version 2.1 all versions FortiDeceptor version 2.0 all versions FortiDeceptor version 1.1 all versions FortiDeceptor version 1.0 all versions FortiMail version 6.4.0 FortiMail version 6.2.1 through 6.2.4 FortiMail version 6.0.0 through 6.0.9 FortiManager version 6.0.0 through 6.0.4 FortiAnalyzer version 6.0.0 through 6.0.4 FortiPortal 4.1 all versions FortiPortal 4.2 all versions FortiPortal 5.0 all versions FortiPortal 5.1 all versions FortiPortal 5.2 all versions FortiPortal 5.3 all versions FortiPortal version 6.0.0 through 6.0.9 FortiSwitch version 6.0.0 through 6.0.7 FortiSwitch version 6.2.0 through 6.2.7 FortiSwitch version 6.4.0 through 6.4.10 FortiSwitch version 7.0.0 through 7.0.4 FortiNAC version 9.4.0 FortiNAC version 9.2.0 through 9.2.5	FortiNAC version 9.1.0 through 9.1.8 FortiNAC all versions 8.8, 8.7, 8.6, 8.5, 8.3 FortiNAC version 9.4.0 through 9.4.1 FortiNAC version 9.2.0 through 9.2.6 FortiOS version 7.2.0 through 7.2.3 FortiOS version 7.0.0 through 7.0.9 FortiOS version 6.4.0 through 6.4.11 FortiOS 6.2 all versions FortiProxy version 7.2.0 through 7.2.1 FortiProxy version 7.0.0 through 7.0.7 FortiProxy version 2.0.0 through 2.0.11 FortiProxy 1.2 all versions FortiProxy 1.1 all versions FortiOS 6.0 all versions FortiOS version 7.0.0 through 7.0.8 FortiOS version 6.2.0 through 6.2.12 FortiProxy version 1.2.0 through 1.2.13 FortiProxy version 1.1.0 through 1.1.6 FortiProxy version 7.2.0 through 7.2.2 FortiProxy version 7.0.0 through 7.0.8 FortiOS version 6.2.3 and above FortiSOAR version 7.3.0 through 7.3.1 FortiWeb version 7.0.0 through 7.0.2 FortiWeb version 6.3.6 through 6.3.20 FortiWeb 6.4 all versions FortiWeb version 6.4.0 through 6.4.1 FortiWeb version 6.3.0 through 6.3.17 FortiWeb all versions 6.2 FortiWeb all versions 6.1 FortiWeb all versions 6.0 FortiRecorder version 6.4.0 through 6.4.3 FortiRecorder all versions 6.0 FortiRecorder all versions 2.7 Note: Impact on FortiProxy 7.0.x, 2.0.x, 1.2.x, 1.1.x is minor as it does not have VDOMs
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-22-488 https://www.fortiguard.com/psirt/FG-IR-22-447 https://www.fortiguard.com/psirt/FG-IR-20-078 https://www.fortiguard.com/psirt/FG-IR-18-232 https://www.fortiguard.com/psirt/FG-IR-22-309 https://www.fortiguard.com/psirt/FG-IR-22-477 https://www.fortiguard.com/psirt/FG-IR-22-369 https://www.fortiguard.com/psirt/FG-IR-22-401 https://www.fortiguard.com/psirt/FG-IR-22-364 https://www.fortiguard.com/psirt/FG-IR-22-388 https://www.fortiguard.com/psirt/FG-IR-23-050 https://www.fortiguard.com/psirt/FG-IR-22-254 https://www.fortiguard.com/psirt/FG-IR-21-218

Affected Product	**IBM**
Severity	**Medium**
Affected Vulnerability	Denial of service vulnerability (CVE-2022-3509, CVE-2022-3171)
Description	IBM has released security updates to address multiple denial of service vulnerabilities that exists in their products. These vulnerabilities allows an attacker to compromise vulnerable systems. **CVE-2022-3509**- The vulnerability exists in protobuf-java core and lite caused by a flaw in parsing procedure for text format data. A remote authenticated attacker could exploit this vulnerability by sending non-repeated embedded messages with repeated or unknown fields to cause long garbage collection pauses. **CVE-2022-3171**- The vulnerability exists in protobuf-java core and lite caused by a flaw in parsing procedure for binary and text format data. A remote authenticated attacker could exploit this vulnerability by sending non-repeated embedded messages with repeated or unknown fields to cause long garbage collection pauses. IBM recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	IBM MQ Version 9.1 LTS, 9.2 LTS, 9.3 LTS IBM MQ Version 9.1 CD, 9.2 CD, 9.3 CD
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6960535

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.