Advisory Alert

Alert Number: **AAA20231011** **Date:** **October 11, 2023**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Microsoft	**Critical**	Multiple Vulnerabilities
FortiGuard	**Critical**	Multiple Vulnerabilities
Citrix	**Critical**	Multiple Vulnerabilities
IBM	**Critical**	Multiple Vulnerabilities
Suse	**High**	Multiple Vulnerabilities
Samba	**High**	Multiple Vulnerabilities
Lenovo	**High**	Multiple Vulnerabilities
FortiGuard	**High, Medium, Low**	Multiple Vulnerabilities
Redhat	**High, Medium**	Multiple Vulnerabilities
Tomcat	**High, Medium**	Multiple Vulnerabilities
HPE	**High, Medium**	Multiple Vulnerabilities
IBM	**High, Medium**	Multiple Vulnerabilities

Description

Affected Product	**Microsoft**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-29348, CVE-2023-35349, CVE-2023-36414, CVE-2023-36415, CVE-2023-36416, CVE-2023-36417, CVE-2023-36418, CVE-2023-36419, CVE-2023-36420, CVE-2023-36429, CVE-2023-36431, CVE-2023-36433, CVE-2023-36434, CVE-2023-36435, CVE-2023-36436, CVE-2023-36438, CVE-2023-36557, CVE-2023-36561, CVE-2023-36563, CVE-2023-36564, CVE-2023-36565, CVE-2023-36566, CVE-2023-36567, CVE-2023-36568, CVE-2023-36569, CVE-2023-36570, CVE-2023-36571, CVE-2023-36572, CVE-2023-36573, CVE-2023-36574, CVE-2023-36575, CVE-2023-36576, CVE-2023-36577, CVE-2023-36578, CVE-2023-36579, CVE-2023-36581, CVE-2023-36582, CVE-2023-36583, CVE-2023-36584, CVE-2023-36585, CVE-2023-36589, CVE-2023-36590, CVE-2023-36591, CVE-2023-36592, CVE-2023-36593, CVE-2023-36594, CVE-2023-36596, CVE-2023-36598, CVE-2023-36602, CVE-2023-36603, CVE-2023-36605, CVE-2023-36606, CVE-2023-36697, CVE-2023-36698, CVE-2023-36701, CVE-2023-36702, CVE-2023-36703, CVE-2023-36704, CVE-2023-36706, CVE-2023-36707, CVE-2023-36709, CVE-2023-36710, CVE-2023-36711, CVE-2023-36712, CVE-2023-36713, CVE-2023-36717, CVE-2023-36718, CVE-2023-36720, CVE-2023-36721, CVE-2023-36722, CVE-2023-36723, CVE-2023-36724, CVE-2023-36725, CVE-2023-36726, CVE-2023-36728, CVE-2023-36729, CVE-2023-36730, CVE-2023-36731, CVE-2023-36732, CVE-2023-36737, CVE-2023-36743, CVE-2023-36776, CVE-2023-36778, CVE-2023-36780, CVE-2023-36785, CVE-2023-36786, CVE-2023-36789, CVE-2023-36790, CVE-2023-36902, CVE-2023-38159, CVE-2023-38166, CVE-2023-38171, CVE-2023-41763, CVE-2023-41765, CVE-2023-41766, CVE-2023-41767, CVE-2023-41768, CVE-2023-41769, CVE-2023-41770, CVE-2023-41771, CVE-2023-41772, CVE-2023-41773, CVE-2023-41774)
Description	Microsoft has released critical security updates for October 2023. This release includes fixes for several vulnerabilities across various Microsoft products. It is highly recommended that you apply these security patches immediately to protect your systems from potential threats.
Affected Products	Windows RDP Windows Message Queuing Azure SDK Microsoft Dynamics SQL Server Azure Real Time Operating System Azure Windows IIS Microsoft QUIC Windows HTML Platform Windows TCP/IP Azure DevOps Microsoft WordPad Microsoft Windows Search Component Microsoft Office Microsoft Common Data Model SDK Windows Deployment Services Windows Kernel Microsoft WDAC OLE DB provider for SQL Windows Mark of the Web (MOTW) Windows Active Template Library Microsoft Graphics Component Windows Remote Procedure Call Windows Named Pipe File System Windows Resilient File System (ReFS) Windows Microsoft DirectMusic Windows DHCP Server Windows Setup Files Cleanup Windows AllJoyn API Microsoft Windows Media Foundation Windows Runtime C++ Template Library Windows Common Log File System Driver Windows TPM Windows Virtual Trusted Platform Module Windows Mixed Reality Developer Tools Windows Error Reporting Active Directory Domain Services Windows Container Manager Service Windows Power Management Service Windows NT OS Kernel Windows IKE Extension Windows Win32K Microsoft Exchange Server Skype for Business Windows Client/Server Runtime Subsystem Windows Layer 2 Tunneling Protocol Client Server Run-time Subsystem (CSRSS)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://msrc.microsoft.com/update-guide/releaseNote/2023-Oct

Affected Product	**FortiGuard**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-34992, CVE-2023-34993)
Description	Fortiguard has released critical security updates for FortiSIEM and FortiWLM. This release includes fixes for Unauthenticated command injection and Remote unauthenticated os command injection vulnerabilities. It is highly recommended that you apply these security patches immediately to protect your systems from potential threats.
Affected Products	FortiSIEM version 7.0.0 FortiSIEM version 6.7.0 through 6.7.5 FortiSIEM version 6.6.0 through 6.6.3 FortiSIEM version 6.5.0 through 6.5.1 FortiSIEM version 6.4.0 through 6.4.2 FortiWLM 8.6.0 through 8.6.5 FortiWLM 8.5.0 through 8.5.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-23-130 https://www.fortiguard.com/psirt/FG-IR-23-140

Affected Product	**Citrix**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-1304, CVE-2023-20588, CVE-2023-34324, CVE-2023-4966, CVE-2023-4967)
Description	Citrix has released a security update addressing multiple vulnerabilities. Exploitation of the most severe vulnerabilities could lead to Sensitive information disclosure, Denial of service. Citrix recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	NetScaler ADC and NetScaler Gateway 14.1 before 14.1-8.50 NetScaler ADC and NetScaler Gateway 13.1 before 13.1-49.15 NetScaler ADC and NetScaler Gateway 13.0 before 13.0-92.19 NetScaler ADC 13.1-FIPS before 13.1-37.164 NetScaler ADC 12.1-FIPS before 12.1-55.300 NetScaler ADC 12.1-NDcPP before 12.1-55.300 Citrix Hypervisor 8.2 CU1 LTSR
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.citrix.com/article/CTX579459/netscaler-adc-and-netscaler-gateway-security-bulletin-for-cve20234966-and-cve20234967 https://support.citrix.com/article/CTX575089/citrix-hypervisor-multiple-security-updates

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-37601, CVE-2016-1000027, CVE-2023-29402, CVE-2023-29405, CVE-2023-29404)
Description	IBM has released security updates addressing multiple vulnerabilities that exists in IBM QRadar and IBM DB2. Exploitation of the most severe vulnerabilities could lead to privilege escalation, sensitive information discloser, arbitrary code execute, heap-based buffer overflow and denial of service. IBM recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	IBM QRadar Use Case Manager App 1.0 - 3.7.0 IBM QRadar Network Packet Capture 7.5.0 - 7.5.0 Update Package 5 IBM QRadar SIEM 7.5.0 - 7.5.0 UP6 IBM Db2 Rest 1.0.0.121-amd64 to 1.0.0.276-amd64 IBM Db2 on Cloud Pak for Data and Db2 Warehouse on Cloud Pak for Data v3.5 through refresh 10 IBM Db2 on Cloud Pak for Data and Db2 Warehouse on Cloud Pak for Data v4.0 through refresh 9 IBM Db2 on Cloud Pak for Data and Db2 Warehouse on Cloud Pak for Data v4.5 through refresh 3 IBM Db2 on Cloud Pak for Data and Db2 Warehouse on Cloud Pak for Data v4.6 through refresh 6 IBM Db2 on Cloud Pak for Data and Db2 Warehouse on Cloud Pak for Data v4.7 through refresh 2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7049126 https://www.ibm.com/support/pages/node/7049129 https://www.ibm.com/support/pages/node/7049133 https://www.ibm.com/support/pages/node/7049434 https://www.ibm.com/support/pages/node/7049435

Affected Product	**Suse**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-1206, CVE-2023-39192, CVE-2023-39193, CVE-2023-39194, CVE-2023-4155, CVE-2023-42753, CVE-2023-42754, CVE-2023-4389, CVE-2023-4622, CVE-2023-4623 CVE-2023-4921, CVE-2023-5345, CVE-2020-36766, CVE-2023-0394, CVE-2023-1192, CVE-2023-1859, CVE-2023-2177, CVE-2023-23454, CVE-2023-40283, CVE-2023-4881, CVE-2023-1077, CVE-2023-2007, CVE-2023-20588, CVE-2023-3772, CVE-2023-4385, CVE-2023-4459)
Description	Suse has released important security updates. These updates address multiple vulnerabilities and enhance the security of your SUSE Linux systems. Suse has recommended that you apply these updates to your systems as soon as possible to safeguard your infrastructure and data.
Affected Products	openSUSE Leap 15.5 SUSE Linux Enterprise High Performance Computing 15 SP5 SUSE Linux Enterprise Live Patching 15-SP5 SUSE Linux Enterprise Micro 5.5 SUSE Linux Enterprise Real Time 15 SP5 SUSE Linux Enterprise Server 12 SP5 ,15 SP5 SUSE Linux Enterprise Server for SAP Applications 12 SP5, 15 SP5 SUSE Real Time Module 15-SP5 SUSE Linux Enterprise High Availability Extension 12 SP5 SUSE Linux Enterprise High Performance Computing 12 SP5 SUSE Linux Enterprise Live Patching 12-SP5 SUSE Linux Enterprise Software Development Kit 12 SP5 SUSE Linux Enterprise Workstation Extension 12 12-SP5 SUSE Linux Enterprise High Availability Extension 15 SP2 SUSE Linux Enterprise High Performance Computing 15 SP2, and 15 SP2 LTSS 15-SP2 SUSE Linux Enterprise Live Patching 15-SP2 SUSE Linux Enterprise Server 15 SP2 , SP2 Business Critical Linux 15-SP2, 15 SP2 LTSS 15-SP2 SUSE Linux Enterprise Server SUSE Linux Enterprise Server for SAP Applications 15 SP2 SUSE Manager Proxy 4.1 SUSE Manager Retail Branch Server 4.1 SUSE Linux Enterprise Real Time 12 SP5 SUSE Linux Enterprise Server 11 SP4 and 11 SP4 LTSS EXTREME CORE 11-SP4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2023/suse-su-20234035-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20234031-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20234030-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20234033-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20234032-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20234028-1/

Affected Product	**Samba**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-3961, CVE-2023-4154, CVE-2023-4091, CVE-2023-42669, CVE-2023-42670)
Description	Samba has released security updates to address multiple vulnerabilities that exist in multiple versions of Samba. **CVE-2023-3961** - The flaw allows SMB clients to connect to existing Unix domain sockets on the file system by exploiting unsanitized pipe names, potentially gaining unauthorized access to sensitive services. **CVE-2023-4154** - The flaw in Samba's implementation of the DirSync control, Active Directory accounts authorized to do some replication, but not to replicate sensitive attributes, can instead replicate critical domain passwords and secrets. **CVE-2023-4091** - The vulnerability exists due to an error in the way SMB protocol implementation in Samba handles file operations. A remote user can request read-only access to files and then truncate them to 0 bytes by opening files with OVERWRITE disposition when using the acl_xattr Samba VFS module with the smb.conf setting "acl_xattr:ignore system acls = yes". **CVE-2023-42669** - The vulnerability exists due to inclusion of the "rpcecho" server into production build, which can call sleep() on AD DC **CVE-2023-42670** - The vulnerability exists due to improper management of internal resources within the application when Samba RPC server is under load, which can lead to incorrect start of servers not built for the AD DC Samba recommended to apply necessary fixes at earliest to avoid issues
Affected Products	CVE-2023-3961 - All versions starting with 4.16.0 CVE-2023-4154 - All versions since Samba 4.0.0 CVE-2023-4091 - All Samba versions CVE-2023-42669 - All versions of Samba since Samba 4.0.0 CVE-2023-42670 - All versions of Samba since Samba 4.16
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.samba.org/samba/security/CVE-2023-3961.html https://www.samba.org/samba/security/CVE-2023-4154.html https://www.samba.org/samba/security/CVE-2023-4091.html https://www.samba.org/samba/security/CVE-2023-42669.html https://www.samba.org/samba/security/CVE-2023-42670.html

Affected Product	**Lenovo**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-5075, CVE-2023-5078, CVE-2023-20594, CVE-2023-20597, CVE-2023-25493, CVE-2023-25494, CVE-2023-43567, CVE-2023-43568, CVE-2023-43569, CVE-2023-43570, CVE-2023-43571, CVE-2023-43572, CVE-2023-43573, CVE-2023-43574, CVE-2023-43575, CVE-2023-43576, CVE-2023-43577, CVE-2023-43578, CVE-2023-43579, CVE-2023-43580, CVE-2023-43581, CVE-2023-45075, CVE-2023-45076, CVE-2023-45077, CVE-2023-45078, CVE-2023-45079)
Description	Multiple vulnerabilities have been identified in BIOS firmware across various vendor products, posing significant risks including information disclosure and arbitrary code execution. Lenovo has released security updates for multiple vulnerabilities affecting a wide range of their products. Attackers exploiting these vulnerabilities could compromise system integrity, leading to severe consequences. It is crucial for users to take immediate actions to mitigate these risks.
Affected Products	Desktop Desktop - All in One Hyperscale Lenovo Notebook Smart Office Storage ThinkAgile ThinkEdge ThinkPad ThinkStation ThinkSystem
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.lenovo.com/us/en/product_security/LEN-141775

Affected Product	**FortiGuard**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-44256, CVE-2023-42782, CVE-2023-37939, CVE-2023-33303, CVE-2022-22298, CVE-2023-36556, CVE-2023-36637, CVE-2023-41838, CVE-2023-42791, CVE-2023-41679, CVE-2023-44249, CVE-2023-42788, CVE-2023-42787, CVE-2023-25607, CVE-2023-41675, CVE-2023-36555, CVE-2023-41841, CVE-2023-37935, CVE-2023-33301, CVE-2023-34989)
Description	Fortiguard has released several important security updates to address vulnerabilities in forti products. This release includes fixes for Server side request forgery, Information disclosure, OS command injection, HTML injection, Arbitrary file deletion, Path traversal, Authorization bypass, HTML injection in SAM, Improper authorization vulnerabilities. It is highly recommended that you apply these security patches immediately to protect your systems from potential threats.
Affected Products	FortiAnalyzer version 7.4.0 FortiAnalyzer version 7.2.0 through 7.2.3 FortiAnalyzer 7.0 all versions FortiAnalyzer 6.4 all versions FortiAnalyzer 6.2 all versions FortiClientMac 7.2.0 through 7.2.1 FortiClientMac 7.0 all versions FortiClientMac 6.4 all versions FortiClientMac 6.2 all versions FortiClientWindows 7.2.0 FortiClientWindows 7.0 all versions FortiClientWindows 6.4 all versions FortiClientWindows 6.2 all versions FortiClientLinux 7.2.0e FortiClientLinux 7.0 all versions FortiClientLinux 6.4 all versions FortiClientLinux 6.2 FortiIsolator version 1.0.0 FortiIsolator version 1.1.0 FortiIsolator version 1.2.0 through 1.2.2 FortiIsolator version 2.0.0 through 2.0.1 FortiIsolator version 2.1.0 through 2.1.2 FortiIsolator version 2.2.0 FortiIsolator version 2.3.0 through 2.3.4 FortiMail 7.2 FortiMail 7.0 FortiMail 6.4 FortiMail 6.2 FortiMail 6.0 FortiAnalyzer 7.2.0 through 7.2.3 FortiAnalyzer 7.0.0 through 7.0.8 FortiAnalyzer 6.4.0 through 6.4.12 FortiAnalyzer 6.2.0 through 6.2.11 FortiManager 7.4.0 FortiManager 7.2.0 through 7.2.3 FortiManager 7.0.0 through 7.0.8 FortiManager 6.4.0 through 6.4.12 FortiManager 6.2.0 through 6.2.11 FortiManager 6.4.1 through 6.4.12 FortiAnalyzer 7.4.0 through 7.4.1 FortiManager version 7.2.0 through 7.2.2 FortiManager version 7.0.0 through 7.0.7 FortiManager version 6.4.0 through 6.4.11 FortiManager 6.2 all versions FortiManager 6.0 all versions FortiManager 7.0 all versions FortiManager 6.4 all versions FortiAnalyzer 7.4.0 FortiAnalyzer 7.2.0 through 7.2.2 FortiAnalyzer 7.0.0 through 7.0.7 FortiAnalyzer 6.4.0 through 6.4.11 FortiAnalyzer 6.0 all versions FortiManager 7.2.0 through 7.2.2 FortiManager 7.0.0 through 7.0.7 FortiManager 6.4.0 through 6.4.11 FortiADC 7.1.0 FortiADC 7.0.0 through 7.0.3 FortiADC 6.2 all versions FortiADC 6.1 all versions FortiADC 6.0 all versions FortiOS version 7.2.0 through 7.2.4 FortiOS version 7.0.0 through 7.0.10 FortiProxy version 7.2.0 through 7.2.2 FortiProxy version 7.0.0 through 7.0.8 FortiOS 7.2.0 through 7.2.4 FortiOS 7.0.0 through 7.0.11 FortiOS 7.4.0 FortiOS 7.2.0 through 7.2.5 FortiOS 7.0.0 through 7.0.12 FortiOS version 7.4.0 FortiWLM version 8.6.5 and below FortiWLM version 8.5.4 and below
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-19-039 https://www.fortiguard.com/psirt/FG-IR-23-221 https://www.fortiguard.com/psirt/FG-IR-22-235 https://www.fortiguard.com/psirt/FG-IR-23-007 https://www.fortiguard.com/psirt/FG-IR-21-233 https://www.fortiguard.com/psirt/FG-IR-23-202 https://www.fortiguard.com/psirt/FG-IR-23-194 https://www.fortiguard.com/psirt/FG-IR-23-169 https://www.fortiguard.com/psirt/FG-IR-23-189 https://www.fortiguard.com/psirt/FG-IR-23-062 https://www.fortiguard.com/psirt/FG-IR-23-201 https://www.fortiguard.com/psirt/FG-IR-23-167 https://www.fortiguard.com/psirt/FG-IR-23-187 https://www.fortiguard.com/psirt/FG-IR-22-352 https://www.fortiguard.com/psirt/FG-IR-23-184 https://www.fortiguard.com/psirt/FG-IR-23-104 https://www.fortiguard.com/psirt/FG-IR-23-318 https://www.fortiguard.com/psirt/FG-IR-23-120 https://www.fortiguard.com/psirt/FG-IR-23-139 https://www.fortiguard.com/psirt/FG-IR-23-141

Affected Product	**Redhat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-4128, CVE-2023-31248, CVE-2023-35001, CVE-2023-35788, CVE-2022-42896, CVE-2023-20593, CVE-2023-3609, CVE-2023-32233, CVE-2020-36558, CVE-2022-2503, CVE-2022-2873, CVE-2022-36879, CVE-2023-0590, CVE-2023-1095, CVE-2023-1206, CVE-2023-2235, CVE-2023-3090, CVE-2023-4004, CVE-2023-1637, CVE-2023-3776)
Description	Red Hat has released several important security updates to address vulnerabilities in various products. It is strongly recommended to apply these updates to your systems to ensure the security and integrity of your Red Hat environment.
Affected Products	Red Hat Enterprise Linux Server 7 x86_64 Red Hat Enterprise Linux for Power, little endian 7 ppc64le Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.0 x86_64 Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.0 ppc64le 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 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 Red Hat Enterprise Linux Server - AUS 8.2 x86_64 Red Hat Enterprise Linux Server - TUS 8.2 x86_64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.0 s390x Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.0 aarch64 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 Red Hat Enterprise Linux for Real Time 7 x86_64 Red Hat Enterprise Linux for Real Time for NFV 7 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 8.6 x86_64 Red Hat Enterprise Linux Server - AUS 8.6 x86_64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 8.6 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 8.6 ppc64le Red Hat Virtualization Host 4 for RHEL 8 x86_64 Red Hat Enterprise Linux Server - TUS 8.6 x86_64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 8.6 aarch64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.6 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.6 x86_64 Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 8.6 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 8.6 ppc64le Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 8.6 aarch64 Red Hat Enterprise Linux Server - AUS 8.4 x86_64 Red Hat Enterprise Linux Server - TUS 8.4 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.4 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.4 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2023:5574 https://access.redhat.com/errata/RHSA-2023:5575 https://access.redhat.com/errata/RHSA-2023:5580 https://access.redhat.com/errata/RHSA-2023:5588 https://access.redhat.com/errata/RHSA-2023:5589 https://access.redhat.com/errata/RHSA-2023:5591 https://access.redhat.com/errata/RHSA-2023:5607 https://access.redhat.com/errata/RHSA-2023:5621 https://access.redhat.com/errata/RHSA-2023:5627 https://access.redhat.com/errata/RHSA-2023:5628

Affected Product	**Tomcat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-45648, CVE-2023-44487, CVE-2023-42795, CVE-2023-42794)
Description	Apache Tomcat has released Security Updates addressing multiple vulnerabilities that exist in their products. **CVE-2023-45648** - Tomcat did not correctly parse HTTP trailer headers, allowing a specially crafted header to be treated as multiple requests. This vulnerability could lead to request smuggling, especially when behind a reverse proxy. **CVE-2023-44487** - Tomcat's HTTP/2 implementation was vulnerable to rapid reset attacks, leading to OutOfMemoryError and potential denial of service. **CVE-2023-42795** - Recycling internal objects improperly could leak information from the current request/response to the next, posing a significant security risk. **CVE-2023-42794** - Tomcat's internal fork of Commons FileUpload had a potential denial of service issue on Windows if a web application failed to close uploaded file streams. Apache Tomcat recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	Apache Tomcat 8.5.94 Apache Tomcat 9.0.81 Apache Tomcat 10.1.14 Apache Tomcat 11.0.0-M12
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.94 https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.81 https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.1.14 https://tomcat.apache.org/security-11.html#Fixed_in_Apache_Tomcat_11.0.0-M12

Affected Product	**HPE**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-0187, CVE-2022-26343, CVE-2022-26837, CVE-2022-32231, CVE-2022-26837, CVE-2021-0187, CVE-2022-32231, CVE-2022-26343)
Description	HPE has released Security Updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities could lead to privilege escalation, remotely exploited to allow desync vulnerability. HPE has recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	HPE ProLiant BL460c Gen10 Server Blade - Prior to 2.76_02-09-2023 HPE Synergy 480 Gen10 Compute Module - Prior to 2.76_02-09-2023 HPE Synergy 660 Gen10 Compute Module - Prior to 2.76_02-09-2023 HPE Synergy 480 Gen10 Plus Compute Module - Prior to 1.72_02-02-2023 HPE Synergy 480 Gen9 Compute Module - Prior to 3.08_01-12-2023 HPE Synergy 660 Gen9 Compute Module - Prior to 3.08_01-12-2023 HPE StoreEasy 1660 Storage - Prior to 1.72_02-02-2023 (U46 ROM Family), - Prior to 2.76_01-18-2023 (U30 ROM Family) HPE StoreEasy 1860 Storage - Prior to 1.72_02-02-2023 (U46 ROM Family), - Prior to 2.76_01-18-2023 (U30 ROM Family) HPE StoreEasy 1460 Storage - Prior to 2.76_02-09-2023 HPE StoreEasy 1560 Storage - Prior to 2.76_02-09-2023 HPE StoreEasy 1660 Expanded Storage - Prior to 2.76_02-09-2023 HPE StoreEasy 1660 Performance Storage - Prior to 2.76_02-09-2023 HPE StoreEasy 1860 Performance Storage - Prior to 2.76_02-09-2023 HPE Storage File Controller - Prior to 2.76_02-09-2023 HPE Storage Performance File Controller - Prior to 2.76_02-09-2023 HPE StoreEasy 1550 Storage - Prior to 3.08_01-12-2023 HPE StoreEasy 1650 Storage - Prior to 3.08_01-12-2023 HPE StoreEasy 1850 Storage - Prior to 3.08_01-12-2023 HPE StoreEasy 3850 Gateway Storage Blade - Prior to 3.08_01-12-2023
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04434en_us https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04426en_us https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbst04539en_us

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-25901, CVE-2023-2142, CVE-2023-0842, CVE-2022-24999, CVE-2022-37603, CVE-2022-38900, CVE-2023-38408, CVE-2022-37434, CVE-2023-0767, CVE-2022-4378, CVE-2022-42703, CVE-2023-0286, CVE-2023-22809, CVE-2023-34981, CVE-2020-13956, CVE-2023-21830, CVE-2023-21843, CVE-2022-3564, CVE-2023-32067, CVE-2023-33201, CVE-2023-28709, CVE-2023-30441, CVE-2023-40367, CVE-2023-34455, CVE-2023-34454, CVE-2023-34453, CVE-2022-40609, CVE-2022-48339, CVE-2023-35116, CVE-2023-20867, CVE-2022-21426, CVE-2023-26048, CVE-2023-26049, CVE-2023-30994, CVE-2023-2828, CVE-2023-34149, CVE-2023-25652, CVE-2023-29007, CVE-2023-32697, CVE-2023-21930, CVE-2023-21967, CVE-2023-21954, CVE-2023-21939, CVE-2023-21968, CVE-2023-21937, CVE-2023-21938, CVE-2023-2597, CVE-2023-2976, CVE-2023-34396, CVE-2023-29403, CVE-2023-30447, CVE-2023-30446, CVE-2023-30443, CVE-2023-30448, CVE-2023-30445, CVE-2023-30449, CVE-2023-23487, CVE-2023-30431, CVE-2023-27869, CVE-2023-27867, CVE-2023-27868, CVE-2023-30442, CVE-2023-29256, CVE-2023-27558, CVE-2023-35012)
Description	IBM has released security updates addressing multiple vulnerabilities that exists in IBM QRadar and IBM DB2. Exploitation of the most severe vulnerabilities could lead to privilege escalation, sensitive information discloser, arbitrary code execute, heap-based buffer overflow and denial of service. IBM recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	IBM QRadar Use Case Manager App 1.0 - 3.7.0 IBM QRadar Network Packet Capture 7.5.0 - 7.5.0 Update Package 5 IBM QRadar SIEM 7.5.0 - 7.5.0 UP6 IBM Db2 Rest 1.0.0.121-amd64 to 1.0.0.276-amd64 IBM Db2 on Cloud Pak for Data and Db2 Warehouse on Cloud Pak for Data v3.5 through refresh 10 IBM Db2 on Cloud Pak for Data and Db2 Warehouse on Cloud Pak for Data v4.0 through refresh 9 IBM Db2 on Cloud Pak for Data and Db2 Warehouse on Cloud Pak for Data v4.5 through refresh 3 IBM Db2 on Cloud Pak for Data and Db2 Warehouse on Cloud Pak for Data v4.6 through refresh 6 IBM Db2 on Cloud Pak for Data and Db2 Warehouse on Cloud Pak for Data v4.7 through refresh 2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7049126 https://www.ibm.com/support/pages/node/7049129 https://www.ibm.com/support/pages/node/7049133 https://www.ibm.com/support/pages/node/7049434 https://www.ibm.com/support/pages/node/7049435

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.