Advisory Alert

Alert Number: AAA20240424 **Date:** April 24, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Red Hat	**High**	Multiple Vulnerabilities
Suse	**High**	Multiple Vulnerabilities
Watchguard	**High**	Multiple Vulnerabilities
IBM	**Medium**	Multiple Vulnerabilities
Ubuntu	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-46915, CVE-2023-1192, CVE-2023-3812, CVE-2023-4459, CVE-2023-7192, CVE-2024-26586, CVE-2024-26602, CVE-2020-36558, CVE-2023-2002, CVE-2023-4622, CVE-2023-4623, CVE-2023-25775)
Description	Red Hat has released security updates addressing Multiple Vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to Denial of Service, Privilege escalation, Out-of-bounds memory access. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
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 7 x86_64 Red Hat Enterprise Linux for Real Time for NFV - Telecommunications Update Service 8.2 x86_64 Red Hat Enterprise Linux for Real Time for NFV 7 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 - Extended Life Cycle Support (for IBM z Systems) 7 s390x Red Hat Enterprise Linux Server - Extended Life Cycle Support 7 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-2024:2008 • https://access.redhat.com/errata/RHSA-2024:2006 • https://access.redhat.com/errata/RHSA-2024:2004 • https://access.redhat.com/errata/RHSA-2024:2003 • https://access.redhat.com/errata/RHSA-2024:1961 • https://access.redhat.com/errata/RHSA-2024:1960

Affected Product	**Suse**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-1086, CVE-2024-26622, CVE-2023-52340, CVE-2023-5717, CVE-2024-1086)
Description	Suse has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to Privilege escalation, Use-after-free-writes, Denial of Service, Heap out-of-bounds writes. Suse advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SUSE Linux Enterprise High Performance Computing 12 SP5, 15 SP3, 15 SP4, 15 SP5 SUSE Linux Enterprise Live Patching 12-SP5, 15 SP3, 15 SP4, 15 SP5 SUSE Linux Enterprise Micro 5.1, 5.2, 5.3, 5.4, 5.5 SUSE Linux Enterprise Real Time 15 SP4, 15 SP5 SUSE Linux Enterprise Server 12 SP5, 15 SP3, 15 SP4, 15 SP5 SUSE Linux Enterprise Server for SAP Applications 12 SP5, 15 SP3, 15 SP4, 15 SP5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2024/suse-su-20241410-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20241409-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20241406-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20241405-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20241401-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20241400-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20241391-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20241390-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20241388-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20241386-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20241380-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20241382-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20241373-1

Affected Product	**Watchguard**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2002-20001, CVE-2022-40735)
Description	Watchguard has released security updates addressing multiple vulnerabilities associated with the Diffie-Hellman Key Agreement Protocol that in turn affect Watchguard products. **CVE-2002-20001** - The vulnerability exists because the application does not properly control consumption of internal resources in the Diffie-Hellman Key Agreement Protocol. A remote attacker can trigger resource exhaustion and perform a denial-of-service (DoS) attack. **CVE-2022-40735** - The vulnerability exists due to the use of unnecessarily expensive calculations. A remote attacker can trigger resource exhaustion and perform a denial-of-service (DoS) attack. Watchguard advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Fireware OS before 12.10 WatchGuard System Manager (WSM) Management Server before 12.10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2024-00008

Affected Product	**IBM**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-27268, CVE-2024-22353, CVE-2023-47731)
Description	IBM has released security updates addressing Multiple Vulnferabilities that exist in their products. **CVE-2024-27268** - IBM WebSphere Application Server Liberty is vulnerable to a denial of service, caused by sending a specially crafted request. A remote attacker could exploit this vulnerability to cause the server to consume memory resources. **CVE-2024-22353** - IBM WebSphere Application Server Liberty is vulnerable to a denial of service, caused by sending a specially crafted request. A remote attacker could exploit this vulnerability to cause the server to consume memory resources. **CVE-2023-47731** - IBM QRadar Suite Software is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM WebSphere Application Server Liberty 17.0.0.3 - 24.0.0.4 IBM WebSphere Application Server versions 8.5 and 9.0 QRadar Suite Software 1.10.12.0 - 1.10.19.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7145809 • https://www.ibm.com/support/pages/node/7145365 • https://www.ibm.com/support/pages/node/7148994

Affected Product	**Ubuntu**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-52600, CVE-2024-26581, CVE-2023-24023, CVE-2023-52603, CVE-2024-26591, CVE-2024-26589)
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to System crash, Null pointer differences. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 22.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://ubuntu.com/security/notices/USN-6742-2 • https://ubuntu.com/security/notices/USN-6743-2

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.