Advisory Alert

Alert Number: **AAA20240924** **Date:** **September 24, 2024**

Document Classification Level **:** Public Circulation Permitted | Public

Information Classification Level **:** TLP: WHITE

Overview

Product	Severity	Vulnerability
SUSE	**High**	Multiple Vulnerabilities
HPE	**High**	Multiple Vulnerabilities
Red Hat	**High**, **Medium**	Multiple Vulnerabilities
Ubuntu	**High**, **Medium**, **Low**	Multiple Vulnerabilities

Description

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-48651, CVE-2022-48662, CVE-2023-52340, CVE-2023-52502, CVE-2023-52772, CVE-2023-52846, CVE-2023-6546, CVE-2024-23307, CVE-2024-26585, CVE-2024-26610, CVE-2024-26622, CVE-2024-26766, CVE-2024-26828, CVE-2024-26852, CVE-2024-26923, CVE-2024-26930, CVE-2024-27398, CVE-2024-35817, CVE-2024-35950, CVE-2024-36921)
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited to cause Integer Overflow, Memory Corruption, Out-Of-Bound, Use-After-Free. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	openSUSE Leap 15.4 openSUSE Leap 15.5 openSUSE Leap 15.6 SUSE Linux Enterprise High Performance Computing 15 SP4 SUSE Linux Enterprise High Performance Computing 15 SP5 SUSE Linux Enterprise Live Patching 15-SP4 SUSE Linux Enterprise Live Patching 15-SP5 SUSE Linux Enterprise Live Patching 15-SP6 SUSE Linux Enterprise Micro 5.3 SUSE Linux Enterprise Micro 5.4 SUSE Linux Enterprise Micro 5.5 SUSE Linux Enterprise Real Time 15 SP4 SUSE Linux Enterprise Real Time 15 SP5 SUSE Linux Enterprise Real Time 15 SP6 SUSE Linux Enterprise Server 15 SP4 SUSE Linux Enterprise Server 15 SP5 SUSE Linux Enterprise Server 15 SP6 SUSE Linux Enterprise Server for SAP Applications 15 SP4 SUSE Linux Enterprise Server for SAP Applications 15 SP5 SUSE Linux Enterprise Server for SAP Applications 15 SP6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2024/suse-su-20243379-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20243375-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20243370-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20243368-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20243365-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20243363-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20243405-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20243361-1/

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-42504, CVE-2024-24980, CVE-2024-22374)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2024-42504 -** A security vulnerability in HPE IceWall Agent products could be exploited remotely to cause a Cross-Site Request Forgery (CSRF) in the login flow. **CVE-2024-24980-** Protection mechanism failure in some 3rd, 4th, and 5th Generation Intel(R) Xeon(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE-2024-22374-** Insufficient control flow management for some Intel(R) Xeon Processors may allow an authenticated user to potentially enable denial of service via local access. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IceWall Federation Agent - Prior to 4.0 (RHEL, Windows) - SAML SP module IceWall Gen11 Enterprise Edition - Prior to 11.0 (RHEL, Windows) - Agent module IceWall Gen11 Standard Edition - Prior to 11.0 (RHEL, Windows) - Agent module IceWall MFA 4.0 Enterprise Edition - Prior to 11.0 (RHEL, Windows) - Agent Plugin (MFA Module) and MFA Proxy modules IceWall MFA 4.0 Standard Edition - Prior to 11.0 (RHEL, Windows) - Agent Plugin (MFA Module) and MFA Proxy modules IceWall SSO Agent Option - Prior to 10.0 (HP-UX) IceWall SSO Dfw - Prior to 11.0 (RHEL, WIndows) HPE SimpliVity 380 Gen11 - Prior to HPE SimpliVity Gen11 Support Pack (SVTSP) v2024_0830
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbmu04711en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04691en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04688en_us&docLocale=en_US

Affected Product	**Red Hat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause NULL pointer dereference, out of bounds access, use-after-free, memory leak, Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 8.8 aarch64, Extended Update Support 9.2 aarch64, Extended Update Support 9.4 aarch64, 8 aarch64, 9 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.2 s390x, Extended Update Support 9.4 s390x, 8 s390x, 9 s390x Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 8.8 ppc64le, Extended Update Support 9.2 ppc64le, Extended Update Support 9.4 ppc64le, 8 ppc64le, 9 ppc64le Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 8.8 x86_64, Extended Update Support 9.2 x86_64, Extended Update Support 9.4 x86_64, 8 x86_64, 9 x86_64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.0 aarch64, 4 years of updates 9.2 aarch64, 4 years of updates 9.4 aarch64, Extended Update Support 8.8 aarch64, Extended Update Support 9.2 aarch64, Extended Update Support 9.4 aarch64, 8 aarch64, 9 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.0 s390x, 4 years of updates 9.2 s390x, 4 years of updates 9.4 s390x, Extended Update Support 8.8 s390x, Extended Update Support 9.2 s390x, Extended Update Support 9.4 s390x, 8 s390x, 9 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 8.8 ppc64le, Extended Update Support 9.2 ppc64le, Extended Update Support 9.4 ppc64le, 8 ppc64le, 9 ppc64le Red Hat Enterprise Linux for Real Time - Telecommunications Update Service 8.4 x86_64, 9 x86_64 Red Hat Enterprise Linux for Real Time for NFV - Telecommunications Update Service 8.4 x86_64, 9 x86_64, 4 years of updates 9.2 x86_64, 4 years of updates 9.4 x86_64 Red Hat Enterprise Linux for Real Time for x86_64 - 4 years of updates 9.2 x86_64, 4 years of updates 9.4 x86_64, Extended Life Cycle Support 7 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 8.8 x86_64, Extended Update Support 9.2 x86_64, Extended Update Support 9.4 x86_64, Update Services for SAP Solutions 8.4 x86_64, Update Services for SAP Solutions 8.8 x86_64, Update Services for SAP Solutions 9.0 x86_64, Update Services for SAP Solutions 9.2 x86_64, Update Services for SAP Solutions 9.4 x86_64, 8 x86_64, 9 x86_64 Red Hat Enterprise Linux Server - AUS 7.7 x86_64, AUS 8.2 x86_64, AUS 8.4 x86_64, AUS 9.2 x86_64, AUS 9.4 x86_64 Red Hat Enterprise Linux Server - Extended Life Cycle Support (for IBM z Systems) 7 s390x, Extended Life Cycle Support 7 x86_64, Extended Life Cycle Support for IBM Power, big endian 7 ppc64, Extended Life Cycle Support for IBM Power, little endian 7 ppc64le Red Hat Enterprise Linux Server - TUS 8.4 x86_64, TUS 8.8 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.4 ppc64le, Update Services for SAP Solutions 8.8 ppc64le, Update Services for SAP Solutions 9.0 ppc64le, Update Services for SAP Solutions 9.2 ppc64le, Update Services for SAP Solutions 9.4 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2024:7005 • https://access.redhat.com/errata/RHSA-2024:7004 • https://access.redhat.com/errata/RHSA-2024:7003 • https://access.redhat.com/errata/RHSA-2024:7002 • https://access.redhat.com/errata/RHSA-2024:7001 • https://access.redhat.com/errata/RHSA-2024:7000 • https://access.redhat.com/errata/RHSA-2024:6999 • https://access.redhat.com/errata/RHSA-2024:6998 • https://access.redhat.com/errata/RHSA-2024:6997 • https://access.redhat.com/errata/RHSA-2024:6995 • https://access.redhat.com/errata/RHSA-2024:6994 • https://access.redhat.com/errata/RHSA-2024:6993 • https://access.redhat.com/errata/RHSA-2024:6992 • https://access.redhat.com/errata/RHSA-2024:6991 • https://access.redhat.com/errata/RHSA-2024:6990 • https://access.redhat.com/errata/RHSA-2024:6964

Affected Product	**Ubuntu**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited to Cause Denial Of Service, NULL Pointer Dereference, Out-Of-Bounds Read, Use-After-Free, Memory Leak Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 22.04 Ubuntu 20.04 Ubuntu 24.04 Ubuntu 18.04 Ubuntu 16.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://ubuntu.com/security/notices/USN-7021-2 • https://ubuntu.com/security/notices/USN-7029-1 • https://ubuntu.com/security/notices/USN-7007-3 • https://ubuntu.com/security/notices/USN-6999-2 • https://ubuntu.com/security/notices/USN-7028-1

Disclaimer

The information provided are gathered from official service provider's websites and portals. FinCSIRT strongly recommends members to apply security fixes as per the given guidelines, following the organization's patch and change management procedures to protect systems from potential threats.