Advisory Alert

Alert Number: **AAA20240522** **Date:** **May 22, 2024**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Ivanti	**Critical**	Multiple SQL Injection Vulnerabilities
IBM	**Critical**	Multiple Vulnerabilities
Veeam	**Critical**	Authentication Bypass Vulnerability
Ivanti	**High**	Multiple Vulnerabilities
HPE	**High**	Multiple Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
VMware Broadcom	**High**	Multiple Vulnerabilities
IBM	**High**, **Medium**	Multiple Vulnerabilities
Veeam	**High**, **Low**	Multiple Vulnerabilities
QNAP	**Medium**	Multiple Vulnerabilities
Juniper	**Medium**	Denial of Service Vulnerability
Ubuntu	**Medium**, **Low**	Multiple Vulnerabilities

Description

Affected Product	**Ivanti**
Severity	**Critical**
Affected Vulnerability	Multiple SQL Injection Vulnerabilities (CVE-2024-29822, CVE-2024-29823, CVE-2024-29824, CVE-2024-29825, CVE-2024-29826, CVE-2024-29827)
Description	Ivanti has issued security updates addressing multiple SQL Injection Vulnerabilities that exist in Ivanti Endpoint Manager. An unspecified SQL Injection vulnerability in Core server of Ivanti EPM 2022 SU5 and prior allows an unauthenticated attacker within the same network to execute arbitrary code. Ivanti advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Core server of Ivanti Endpoint Manager 2022 SU5 and prior
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://forums.ivanti.com/s/article/Security-Advisory-May-2024?language=en_US

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-1996, CVE-2023-42282)
Description	IBM has issued security updates addressing multiple vulnerabilities that exist in IBM Storage Fusion products. **CVE-2022-1996** - go-restful could allow a remote attacker to bypass security restrictions, caused by improper regular expression implementation in the CORS Filter feature. By sending a specially-crafted request using the AllowedDomains parameter, an attacker could exploit this vulnerability to break CORS policy and allow any page to make requests. **CVE-2023-42282** - Node.js IP package could allow a remote attacker to execute arbitrary code on the system, caused by a server-side request forgery flaw in the ip.isPublic() function. By sending a specially crafted request using a hexadecimal representation of a private IP address, an attacker could exploit this vulnerability to execute arbitrary code on the system and obtain sensitive information. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Storage Fusion versions 2.3.0 - 2.7.1 and versions 2.5.0 - 2.7.2 IBM Storage Fusion HCI versions 2.5.2 - 2.7.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7154517 • https://www.ibm.com/support/pages/node/7154515 • https://www.ibm.com/support/pages/node/7154516

Affected Product	**Veeam**
Severity	**Critical**
Affected Vulnerability	Authentication Bypass Vulnerability (CVE-2024-29849)
Description	Veeam has issued security updates addressing an Authentication Bypass Vulnerability that exists in Veeam Backup Enterprise Manager. This vulnerability allows an unauthenticated attacker to log in to the Veeam Backup Enterprise Manager web interface as any user. Veeam advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Veeam Backup & Replication versions 5.0, 6.1, 6.5, 7.0, 8.0, 9.0, 9.5, 10, 11, 12, 12.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.veeam.com/kb4581

Affected Product	**Ivanti**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-29848, CVE-2024-22059, CVE-2024-22060, CVE-2023-38551, CVE-2023-38042, CVE-2023-46810, CVE-2024-29828, CVE-2024-29829, CVE-2024-29830, CVE-2024-29846)
Description	Ivanti has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Denial of Service, SQL Injection, Authentication Bypass, Cross-site Scripting, Information Disclosure, Privilege Escalation. Ivanti advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ivanti Avalanche before 6.4.x Ivanti Neurons for ITSM Ivanti Connect Secure version 9.x, 22.x Ivanti Secure Access Client for Windows Ivanti Endpoint Manager 2022 SU5 Avalanche versions before 6.4.3.602
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://forums.ivanti.com/s/article/Security-Advisory-May-2024?language=en_US • https://forums.ivanti.com/s/article/Avalanche-6-4-3-602-additional-security-hardening-and-CVE-fixed?language=en_US

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-26304, CVE-2024-26305, CVE-2024-33511, CVE-2024-33512, CVE-2024-33513, CVE-2024-33514, CVE-2024-33515, CVE-2024-33516, CVE-2024-33517, CVE-2024-33518)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Arbitrary Code Execution and Denial of Service. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE Aruba Networking • Mobility Conductor (formerly Mobility Master) • Mobility Controllers • WLAN Gateways and SD-WAN Gateways managed by Aruba Central Above Products running on below software versions • ArubaOS 10.5.x.x: versions 10.5.1.0 and below • ArubaOS 10.4.x.x: versions 10.4.1.0 and below • ArubaOS 8.11.x.x: versions 8.11.2.1 and below • ArubaOS 8.10.x.x: versions 8.10.0.10 and below
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04640en_us&docLocale=en_US

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-41678, CVE-2023-6378, CVE-2023-6481, CVE-2023-6717, CVE-2023-44981, CVE-2024-1132, CVE-2024-1249, CVE-2024-22259, CVE-2024-29025, CVE-2024-29131, CVE-2024-29133)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in Red Hat JBoss Middleware. These vulnerabilities could be exploited by malicious users to cause Remote Code Execution, Distributed Denial of Service conditions, Path Traversal, Authorization Bypass. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat JBoss Middleware - Red Hat AMQ Broker versions prior to 7.12.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2024:2945

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Denial of Service, Memory Corruption, Information Disclosure, Use-after-free conditions. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	openSUSE Leap 15.3, 15.4, 15.5 SUSE Linux Enterprise High Availability Extension 12 SP5 SUSE Linux Enterprise High Performance Computing 12 SP5, 15 SP2, 15 SP3, 15 SP4, 15 SP5 SUSE Linux Enterprise Live Patching 12-SP5, 15-SP2, 15-SP3, 15-SP4, 15-SP5 SUSE Linux Enterprise Micro 5.1 - 5.5 SUSE Linux Enterprise Real Time 15 SP4, 15 SP5 SUSE Linux Enterprise Server 12 SP5, 15 SP2, 15 SP3, 15 SP4, 15 SP5 SUSE Linux Enterprise Server for SAP Applications 12 SP5, 15 SP2, 15 SP3, 15 SP4, 15 SP5 SUSE Linux Enterprise Software Development Kit 12 SP5 SUSE Linux Enterprise Workstation Extension 12 12-SP5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2024/suse-su-20241709-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20241711-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20241712-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20241719-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20241720-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20241713-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20241723-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20241726-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20241730-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20241731-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20241732-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20241729-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20241648-2/ • https://www.suse.com/support/update/announcement/2024/suse-su-20241735-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20241736-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20241738-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20241739-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20241740-1/

Affected Product	**VMware Broadcom**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-22273, CVE-2024-22274, CVE-2024-22275)
Description	Broadcom has released security updates addressing multiple vulnerabilities that exist in VMware products. **CVE-2024-22273** - A malicious actor with access to a virtual machine with storage controllers enabled may exploit this issue to create a denial of service condition or execute code on the hypervisor from a virtual machine in conjunction with other issues. **CVE-2024-22274** - A malicious actor with administrative privileges on the vCenter appliance shell may exploit this issue to run arbitrary commands on the underlying operating system. **CVE-2024-22275** - A malicious actor with administrative privileges on the vCenter appliance shell may exploit this issue to partially read arbitrary files containing sensitive data. Broadcom advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	VMware ESXi 7.0, 8.0 VMware Workstation 17.x VMware Fusion 13.x on MacOS VMware Cloud Foundation (ESXi) 4.x, 5.x VMware vCenter Server 7.0, 8.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/security-advisories/0/24308

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-22354, CVE-2023-50313)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in IBM WebSphere products. **CVE-2024-22354** - IBM WebSphere Application Server and IBM WebSphere Application Server Liberty are vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information, consume memory resources, or to conduct a server-side request forgery attack. **CVE-2023-50313** - IBM WebSphere Application Server could provide weaker than expected security for outbound TLS connections caused by a failure to honor user configuration. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM WebSphere Application Server versions 8.5 and 9.0 IBM WebSphere Application Server Liberty versions 17.0.0.3 - 24.0.0.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7145620 • https://www.ibm.com/support/pages/node/7148426

Affected Product	**Veeam**
Severity	**High**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-29850, CVE-2024-29851, CVE-2024-29852, CVE-2024-29853)
Description	Veeam has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Information Disclosure, Credential Theft, Local Privilege Escalation and NTLM Relay Attack. Veeam advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Veeam Backup & Replication versions 5.0, 6.1, 6.5, 7.0, 8.0, 9.0, 9.5, 10, 11, 12, 12.1 Veeam Agent for Microsoft Windows 2.0, 3.0.2, 4.0, 5.0, 6.0, 6.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.veeam.com/kb4581 • https://www.veeam.com/kb4582

Affected Product	**QNAP**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-21902, CVE-2024-27127, CVE-2024-27128, CVE-2024-27129, CVE-2024-27130)
Description	QNAP has released security updates addressing multiple vulnerabilities that exist in QNAP operating systems. These vulnerabilities could be exploited by malicious users to cause Improper Access Control and Arbitrary Code Execution. QNAP advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	QTS versions 5.1.x QuTS hero versions h5.1.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.qnap.com/en/security-advisory/qsa-24-23

Affected Product	**Juniper**
Severity	**Medium**
Affected Vulnerability	Denial of Service Vulnerability (CVE-2024-30402)
Description	Juniper has released security updates addressing a Denial of Service Vulnerability that exists in Junos OS and Junos OS Evolved. **CVE-2024-30402** - An Improper Check for Unusual or Exceptional Conditions vulnerability in the Layer 2 Address Learning Daemon (l2ald) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, adjacent attacker to cause a Denial of Service. Juniper advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Junos OS: • All versions earlier than 20.4R3-S10 • 21.2 versions earlier than 21.2R3-S7 • 21.4 versions earlier than 21.4R3-S5 • 22.1 versions earlier than 22.1R3-S4 • 22.2 versions earlier than 22.2R3-S3 • 22.3 versions earlier than 22.3R3-S1 • 22.4 versions earlier than 22.4R3 • 23.2 versions earlier than 23.2R1-S2, 23.2R2 Junos OS Evolved: • All versions earlier than 21.4R3-S5-EVO • 22.1-EVO versions earlier than 22.1R3-S4-EVO • 22.2-EVO versions earlier than 22.2R3-S3-EVO • 22.3-EVO versions earlier than 22.3R3-S1-EVO • 22.4-EVO versions earlier than 22.4R3-EVO • 23.2-EVO versions earlier than 23.2R2-EVO
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://supportportal.juniper.net/s/article/2024-04-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-The-l2ald-crashes-on-receiving-telemetry-messages-from-a-specific-subscription-CVE-2024-30402?language=en_US

Affected Product	**Ubuntu**
Severity	**Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-26622, CVE-2023-52530, CVE-2023-47233)
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in Ubuntu Linux kernel. **CVE-2024-26622** - In the Linux kernel, fix UAF write bug in tomoyo_write_control() Since tomoyo_write_control() updates head->write_buf when write() of long lines is requested, we need to fetch head->write_buf after head->io_sem is held. Otherwise, concurrent write() requests can cause use-after-free-write and double-free problems. **CVE-2023-52530** - In the Linux kernel, wifi: mac80211: fix potential key use-after-free When ieee80211_key_link() is called by ieee80211_gtk_rekey_add() but returns 0 due to KRACK protection (identical key reinstall), ieee80211_gtk_rekey_add() will still return a pointer into the key, in a potential use-after-free. **CVE-2023-47233** - Broadcom FullMAC WLAN driver in the Linux kernel contained a race condition during device removal, leading to a use-after-free vulnerability. A physically proximate attacker could possibly use this to cause a denial of service. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 22.04 Ubuntu 20.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-6775-2

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.