Advisory Alert

Alert Number: AAA20240920 **Date:** September 20, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Ivanti	**Critical**	Path Traversal Vulnerability
SUSE	**High**	Multiple Vulnerabilities
Hitachi	**High**, **Medium**, **Low**	Multiple Vulnerabilities
IBM	**Low**	Multiple Vulnerabilities

Description

Affected Product	**Ivanti**
Severity	**Critical**
Affected Vulnerability	Path Traversal Vulnerability (CVE-2024-8963)
Description	Ivanti has released security updates addressing a Path Traversal Vulnerability that exists in Ivanti Cloud Service Appliance before 4.6 Patch 519 allows a remote unauthenticated attacker to access restricted functionality.. Ivanti advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ivanti Cloud Services Appliance (CSA): before 4.6 Patch 519
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-CSA-4-6-Cloud-Services-Appliance-CVE-2024-8963?language=en_US

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-48651, CVE-2022-48662, CVE-2023-52502, CVE-2023-52846, CVE-2023-6546, CVE-2024-23307, CVE-2024-26610, CVE-2024-26828, CVE-2024-26852, CVE-2024-26923, CVE-2024-26930, CVE-2024-27398, CVE-2024-35817, CVE-2024-35950, CVE-2024-40909)
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited to cause memory leakage, use-after-free conditions, race conditions. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	openSUSE Leap 15.5 openSUSE Leap 15.6 openSUSE Leap Micro 5.5 SUSE Linux Enterprise High Performance Computing 15 SP5 SUSE Linux Enterprise Live Patching 15-SP5 SUSE Linux Enterprise Live Patching 15-SP6 SUSE Linux Enterprise Micro 5.5 SUSE Linux Enterprise Real Time 15 SP5 SUSE Linux Enterprise Real Time 15 SP6 SUSE Linux Enterprise Server 15 SP5 SUSE Linux Enterprise Server 15 SP6 SUSE Linux Enterprise Server for SAP Applications 15 SP5 SUSE Linux Enterprise Server for SAP Applications 15 SP6 SUSE Real Time Module 15-SP5 SUSE Real Time Module 15-SP6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2024/suse-su-20243349-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20243348-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20243347-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20243334-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20243338-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20243337-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20243336-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20243322-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20243321-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20243320-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20243319-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20243318-1/

Affected Product	**Hitachi**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	Hitachi has released security updates addressing multiple vulnerabilities that exist in Hitachi Virtual Storage Platform. These vulnerabilities could be exploited by malicious users to cause Out-Of-Bound Write , Remote Code Execution , Secure Boot Bypass, Denial Of Service, Privilege Escalation Hitachi advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Hitachi Virtual Storage Platform 5200, 5600, 5200H, 5600H Hitachi Virtual Storage Platform 5100, 5500, 5100H, 5500H Hitachi Virtual Storage Platform G1000, G1500 Hitachi Virtual Storage Platform F1500 Hitachi Virtual Storage Platform VX7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.hitachi.com/products/it/storage-solutions/sec_info/2024/08.html

Affected Product	**IBM**
Severity	**Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-40681, CVE-2024-40680, CVE-2024-2511, CVE-2024-21085)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in IBM WebSphere Remote Server. These vulnerabilities could be exploited by malicious users to cause Denial of Service, Security Bypass IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM WebSphere Remote Server 9.0, 9.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7168962

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.