Advisory Alert

Alert Number: **AAA20240321** **Date:** **March 21, 2024**

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

Information Classification Level **:** TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
IBM	**Critical**	Multiple Vulnerabilities
Ivanti	**Critical**	Multiple Vulnerabilities
F5	**High**	Denial of Service Vulnerability
HPE	**High**	Local Escalation of Privilege Vulnerability
IBM	**High, Medium, Low**	Multiple Vulnerabilities
Ubuntu	**High, Medium, Low**	Multiple Vulnerabilities

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell has issued security updates addressing multiple vulnerabilities that exist in Dell EMC VxRail Appliance. These vulnerabilities could be exploited by malicious users to compromise the affected system. Dell advises to apply security fixes at your earliest to protect your systems from potential threats.
Affected Products	Dell EMC VxRail Appliance versions prior to 8.0.120
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000223344/dsa-2024-147-dell-vxrail-security-update-for-multiple-third-party-component-vulnerabilities

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-51385, CVE-2023-45871, CVE-2022-22980, CVE-2023-52071)
Description	IBM has issued security updates by addressing multiple vulnerabilities within third-party components that impact IBM Spectrum Protect Plus. These vulnerabilities could be exploited by malicious users to cause Arbitrary Code Execution and Denial of Service. IBM advises to apply security fixes at your earliest to protect your systems from potential threats.
Affected Products	IBM Storage Protect Plus Server v10.1 - v10.1.16
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7144861

Affected Product	**Ivanti**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-46808, CVE-2023-41724)
Description	Ivanti has issued security updates addressing multiple vulnerabilities that exist in Ivanti Standalone Sentry and Neurons for ITSM. These vulnerabilities could be exploited by malicious users to cause Remote Code Execution and Authenticated Remote File Write condition. **CVE-2023-46808** - An authenticated remote user can perform file writes to ITSM server. Successful exploitation can be used to write files to sensitive directories which may allow attackers execution of commands in the context of web application's user. **CVE-2023-41724** - An unauthenticated threat actor can execute arbitrary commands on the underlying operating system of the appliance within the same physical or logical network. Ivanti advises to apply security fixes at your earliest to protect your systems from potential threats.
Affected Products	Ivanti Standalone Sentry v9.19.0 and prior versions Ivanti Neurons for ITSM v2023.3 and prior versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://forums.ivanti.com/s/article/CVE-2023-41724-Remote-Code-Execution-for-Ivanti-Standalone-Sentry?language=en_US https://forums.ivanti.com/s/article/SA-CVE-2023-46808-Authenticated-Remote-File-Write-for-Ivanti-Neurons-for-ITSM?language=en_US

Affected Product	**F5**
Severity	**High**
Affected Vulnerability	Denial of Service Vulnerability (CVE-2022-23308)
Description	F5 has released a security update addressing a vulnerability that exists in BIG-IP modules and F5OS. The security impact of xmlGetID() returning a pointer to freed memory depends on the application and mostly results in Denial of Service. F5 advises to apply security fixes at your earliest to protect your systems from potential threats.
Affected Products	BIG-IP versions 17.0.0, 16.1.0 - 16.1.3, 15.1.0 - 15.1.7 F5OS-C versions 1.5.0 - 1.5.1, 1.3.0 - 1.3.2, 1.2.0 - 1.2.2, 1.1.0 - 1.1.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K32760744

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	Local Escalation of Privilege Vulnerability (CVE-2023-22655)
Description	HPE has released a security update addressing a vulnerability that exists in HPE StoreEasy Servers. These vulnerabilities could be exploited locally by malicious users to allow escalation of privilege. HPE advises to apply security fixes at your earliest to protect your systems from potential threats.
Affected Products	HPE StoreEasy 1660 Storage - Prior to v2.00_03-06-2024 HPE StoreEasy 1860 Storage - Prior to v2.00_03-06-2024
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbst04611en_us

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-1838, CVE-2022-36402, CVE-2021-41079, CVE-2022-22971 , CVE-2023-42753, CVE-2023-28487, CVE-2022-22978, CVE-2024-0646, CVE-2023-6606, CVE-2023-5633, CVE-2023-47715, CVE-2023-2176, CVE-2021-3923, CVE-2023-2248, CVE-2023-26545, CVE-2023-6610, CVE-2023-2162, CVE-2023-51042, CVE-2023-38409, CVE-2022-3545, CVE-2023-2166, CVE-2023-3609, CVE-2023-1074, CVE-2023-2269, CVE-2023-6536, CVE-2023-28486, CVE-2023-1075, CVE-2023-23455, CVE-2023-1192, CVE-2023-4622, CVE-2023-5717, CVE-2023-45862, CVE-2021-42340, CVE-2023-46813, CVE-2023-4921, CVE-2023-42465, CVE-2021-22096, CVE-2022-3594, CVE-2023-1382, CVE-2023-6535, CVE-2022-25762, CVE-2022-22950, CVE-2022-27772, CVE-2023-0597, CVE-2022-45869, CVE-2023-4623, CVE-2022-38457, CVE-2023-33203, CVE-2022-22976, CVE-2023-3812, CVE-2022-3640, CVE-2024-0443, CVE-2023-6817, CVE-2022-28388, CVE-2024-27277, CVE-2023-3567, CVE-2021-22060, CVE-2022-22970, CVE-2023-4207, CVE-2023-48795, CVE-2023-40283, CVE-2023-29986, CVE-2022-29885, CVE-2022-31690, CVE-2023-3772, CVE-2023-52071, CVE-2024-0853, CVE-2023-47745, CVE-2023-4218, CVE-2023-44487, CVE-2023-39976, CVE-2024-25016)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in IBM Spectrum Protect Plus and IBM WebSphere Remote Server. These vulnerabilities could be exploited by malicious users to cause Sensitive Information Disclosure, Privilege Escalation, Arbitrary Command Execution, Denial of Service and security restriction bypass. IBM recommends to apply security fixes at your earliest to protect your systems from potential threats.
Affected Products	IBM Storage Protect Plus Server v10.1 - v10.1.16 IBM WebSphere Remote Server v9.0 and v9.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7144861 https://www.ibm.com/support/pages/node/7144350

Affected Product	**Ubuntu**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-24855, CVE-2023-23004, CVE-2024-1086, CVE-2023-23000, CVE-2024-26597, CVE-2024-1085, CVE-2024-26599, CVE-2023-6039, CVE-2023-32247)
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in Ubuntu Linux kernel. These vulnerabilities could be exploited by malicious users to cause Arbitrary Command Execution and Denial of Service or system crash. Ubuntu recommends to apply security fixes at your earliest to protect your systems from potential threats.
Affected Products	Ubuntu 23.10 Ubuntu 22.04 Ubuntu 20.04 Ubuntu 18.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-6702-2 https://ubuntu.com/security/notices/USN-6707-1 https://ubuntu.com/security/notices/USN-6706-1 https://ubuntu.com/security/notices/USN-6704-1

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.