Advisory Alert

Alert Number: AAA20240816 **Date:** August 16, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
IBM	**Critical**	Prototype Pollution Vulnerability
SUSE	**High**	Multiple Vulnerabilities
Intel	**High**, Medium	Multiple Vulnerabilities
IBM	**High**, Medium, Low	Multiple Vulnerabilities

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell has released security updates addressing multiple vulnerabilities that exist in third party products that in turn affect Dell products. These vulnerabilities could be exploited by malicious users to compromise the affected system. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Dell EMC VxRail Appliance 8.0.x versions prior to 8.0.300
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000227832/dsa-2024-341-security-update-for-dell-vxrail-8-0-300-multiple-third-party-component-vulnerabilities

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Prototype Pollution Vulnerability (CVE-2024-39008)
Description	IBM has released security updates addressing a Prototype Pollution Vulnerability that exists in their products. By sending a specially crafted request, an attacker could exploit this vulnerability to execute arbitrary code or cause a denial of service. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Cloud Pak for Security 1.10.0.0 - 1.10.11.0 QRadar Suite Software 1.10.12.0 - 1.10.23.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7165488

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 compromise the affected systems. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	openSUSE Leap 15.4 SUSE Linux Enterprise Desktop 15 SP4 LTSS 15-SP4 SUSE Linux Enterprise High Availability Extension 15 SP2, 15 SP4 SUSE Linux Enterprise High Performance Computing 15 SP2, 15 SP4 SUSE Linux Enterprise High Performance Computing 15 SP2 LTSS 15-SP2 SUSE Linux Enterprise High Performance Computing ESPOS 15 SP4 SUSE Linux Enterprise High Performance Computing LTSS 15 SP4 SUSE Linux Enterprise Live Patching 15-SP2, 15-SP4 SUSE Linux Enterprise Micro 5.3, 5.4 SUSE Linux Enterprise Micro for Rancher 5.3, 5.4 SUSE Linux Enterprise Real Time 15 SP4 SUSE Linux Enterprise Server 15 SP2, 15 SP4 SUSE Linux Enterprise Server 15 SP2 Business Critical Linux 15-SP2 SUSE Linux Enterprise Server 15 SP2 LTSS 15-SP2, 15 SP4 LTSS 15-SP4 SUSE Linux Enterprise Server for SAP Applications 15 SP2, 15 SP4 SUSE Manager Proxy 4.1, 4.3 SUSE Manager Proxy 4.3 SUSE Manager Retail Branch Server 4.1, 4.3 SUSE Manager Server 4.1, 4.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2024/suse-su-20242923-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20242929-1

Affected Product	**Intel**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities
Description	Intel has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited to cause Privilege Escalation, Denial of Service, Information Disclosure. Intel advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00790.html • https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00918.html • https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00999.html • https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01010.html • https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01022.html • https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01038.html • https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01046.html • https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01057.html • https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01070.html • https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01072.html • https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01073.html • https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01078.html • https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01083.html • https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01089.html • https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01094.html • https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01100.html • https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01106.html • https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01114.html • https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01115.html • https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01116.html • https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01117.html • https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01118.html • https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01121.html • https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01128.html • https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01129.html • https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01164.html • https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01172.html

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-35153, CVE-2024-28176,CVE-2024-34064,CVE-2024-3651,CVE-2024-25024,CVE-2024-37168,CVE-2024-30260,CVE-2024-30261,CVE-2024-28799,CVE-2024-29415)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited to cause Denial of Service, Cross-site Scripting, Sensitive information Disclosure, Security restriction Bypass. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Cloud Pak for Security 1.10.0.0 - 1.10.11.0 QRadar Suite Software 1.10.12.0 - 1.10.23.0 IBM WebSphere Remote Server - Product Family 9.1, 9.0, 8.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7165614 • https://www.ibm.com/support/pages/node/7165488

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.