Advisory Alert

Alert Number: **AAA20240715** **Date:** **July 15, 2024**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
IBM	**Critical**	Sandbox Bypass Flaw
Check Point	**High**	Remote Code Execution vulnerability
Juniper	**High**	Denial of Service Vulnerability
SUSE	**High**	Multiple Vulnerabilities
VMware Broadcom	**High**	Multiple Vulnerabilities
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 released security updates addressing multiple vulnerabilities that exist in their 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	Integrated Data Protection Appliance (PowerProtect DP Series) versions 2.7.4 and prior
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000220651/dsa-2023-416-security-update-for-dell-powerprotect-dp-series-appliance-idpa-infrastructure-for-multiple-vulnerabilities

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Sandbox Bypass Flaw (CVE-2020-13936)
Description	IBM has released security updates addressing a Sandbox Bypass Flaw that exists in IBM QRadar SIEM. Apache Velocity which is used by QRadar SIEM, could allow a remote attacker to execute arbitrary code on the system, caused by a sandbox bypass flaw. By modifying the Velocity templates, an attacker could exploit this vulnerability to execute arbitrary code with the same privileges as the account running the Servlet container. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM QRadar SIEM version 7.5 - 7.5.0 UP8 IF03
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7160134

Affected Product	**Check Point**
Severity	**High**
Affected Vulnerability	Remote Code Execution vulnerability (CVE-2024-6387)
Description	Check Point has released security updates addressing a security regression in the OpenSSH server which affects Check Point products. Remote Code Execution vulnerability in the OpenSSH server (sshd) in glibc-based Linux systems can cause an unauthenticated RCE that grants full root access. Check Point advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Quantum Spark appliances that run the R81.10.x firmware versions : 1500, 1570R, 1575R, 1595R, 1600, 1800, 1900, 2000
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.checkpoint.com/results/sk/sk182459

Affected Product	**Juniper**
Severity	**High**
Affected Vulnerability	Denial of Service (CVE-2024-39549)
Description	Juniper has released security updates addressing a Denial of Service Vulnerability that exists in Junos OS and Junos OS Evolved. A Missing Release of Memory after Effective Lifetime vulnerability in the routing process daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an attacker to send a malformed BGP Path attribute update which allocates memory used to log the bad path attribute. This memory is not properly freed in all circumstances, leading to a Denial of Service (DoS). Juniper advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Junos OS: • All versions before 21.2R3-S8 • From 21.4 before 21.4R3-S8 • From 22.2 before 22.2R3-S4 • From 22.3 before 22.3R3-S3 • From 22.4 before 22.4R3-S3 • From 23.2 before 23.2R2-S1 • From 23.4 before 23.4R1-S2, 23.4R2 • From 24.2 before 24.2R2-EVO Junos OS Evolved: • All versions before 21.2R3-S8-EVO • From 21.4 before 21.4R3-S8-EVO • From 22.2 before 22.2R3-S4-EVO • From 22.3 before 22.3R3-S3-EVO • From 22.4 before 22.4R3-S3-EVO • From 23.2 before 23.2R2-S1-EVO • From 23.4 before 23.4R1-S2, 23.4R2 • From 24.2 before 24.2R2-EVO
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://supportportal.juniper.net/s/article/2024-07-Security-Bulletin-Junos-OS-Receipt-of-malformed-BGP-path-attributes-leads-to-a-memory-leak-CVE-2024-39549?language=en_US

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-23307, CVE-2024-26828, CVE-2024-26923, CVE-2024-26930, CVE-2024-26852, CVE-2022-48651, CVE-2024-26610, CVE-2024-26766, CVE-2023-52502, CVE-2023-6546)
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to Local Privilege Escalation, Memory Corruption, use-after-free, out-of-bound conditions. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	openSUSE Leap 15.4, 15.5 SUSE Linux Enterprise High Performance Computing 15 SP4, 15 SP5 SUSE Linux Enterprise Live Patching 15-SP4, 15-SP5 SUSE Linux Enterprise Micro 5.3, 5.4, 5.5 SUSE Linux Enterprise Real Time 15 SP4, 15 SP5 SUSE Linux Enterprise Server 15 SP4, 15 SP5 SUSE Linux Enterprise Server for SAP Applications 15 SP4, 15 SP5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2024/suse-su-20242437-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20242449-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20242448-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20242447-1/

Affected Product	**VMware Broadcom**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-22264, CVE-2024-22266)
Description	Broadcom has released security updates addressing multiple vulnerabilities that exist in VMware products. **CVE-2024-22264** - VMware Avi Load Balancer contains a privilege escalation vulnerability. A malicious actor with admin privileges on VMware Avi Load Balancer can create, modify, execute and delete files as a root user on the host system. **CVE-2024-22266** - VMware Avi Load Balancer contains an information disclosure vulnerability. A malicious actor with access to the system logs can view cloud connection credentials in plaintext. Broadcom advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	VMware Avi Load Balancer versions 30.x.x and 22.1.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24219

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-25193, CVE-2023-43804, CVE-2023-45803, CVE-2023-31122, CVE-2023-45802, CVE-2019-11358, CVE-2020-11023, CVE-2020-11022, CVE-2020-23064, CVE-2023-29483, CVE-2023-3635, CVE-2024-33599, CVE-2024-3019, CVE-2023-31484, CVE-2024-25062, CVE-2021-40153, CVE-2021-41072, CVE-2020-15778, CVE-2022-3287, CVE-2024-26458, CVE-2024-26461, CVE-2024-28834, CVE-2024-30172, CVE-2024-2961, CVE-2024-33600, CVE-2024-33601, CVE-2024-33602, CVE-2023-6004, CVE-2023-6918, CVE-2023-6597, CVE-2024-0450, CVE-2024-28182, CVE-2024-29857, CVE-2024-30171, CVE-2020-13956)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in IBM QRadar SIEM. Exploitation of these vulnerabilities may lead to Denial of Service, Sensitive Information Disclosure, Arbitrary Command Execution, Memory Corruption. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM QRadar SIEM versions - 7.5 - 7.5.0 UP8
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7160134 • https://www.ibm.com/support/pages/node/7160139

Affected Product	**Ubuntu**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in Ubuntu Linux kernel. Exploitation of these vulnerabilities may lead to Denial of Service, Information Disclosure, Memory Corruption, Code Execution. Ubuntu advises to apply security fixes at your earliest to protect 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-6895-1 • https://ubuntu.com/security/notices/USN-6896-1

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.