Advisory Alert

Alert Number: AAA20240702 **Date:** July 2, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
WatchGuard	**Critical**	Race Condition Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
IBM	**High**, **Medium**	Multiple Vulnerabilities
Cisco	**Medium**	Command Injection Vulnerability
Dell	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**WatchGuard**
Severity	**Critical**
Affected Vulnerability	Race Condition Vulnerability (CVE-2024-6387)
Description	WatchGuard has released security updates addressing a Race Condition Vulnerability that exists in WatchGuard Fireware OS. An unauthenticated attacker could exploit this vulnerability to execute arbitrary code with privileged permissions on affected systems. WatchGuard advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	WatchGuard Fireware OS Running On Firebox : • XTM 1500 and 2520 XTM1520-RP, XTM1525-RP, XTM2520 • Firebox T (2nd Gen) T15, T15-W, T35, T35-W, T35-R, T55, T55-W, T70 • Firebox T (1st Gen) T10, T10-W, T10-D, T30, T30-W, T50, T50-W • Firebox T (3rd Gen) T20, T20-W, T40, T40-W, T80 • Firebox M (2nd Gen) M270, M370, M470, M570, M670 • Firebox M (3rd Gen) M290, M390, M590, M690, M4800, M5800 • Firebox M (1st Gen) M200, M300, M400, M440, M500 • FireboxV Small, Medium, Large, XLarge • FireboxCloud Small, Medium, Large, XLarge • XTMv Small, Medium, Large, Datacenter • Firebox T (4th Gen) NV5, T25, T45, T85 WatchGuard Fireware OS Running On Secure Wi-Fi : • Wi-Fi 6 AP130, AP330, AP430CR, AP432 • Wi-Fi 4 & 5 AP322, AP420, AP125, AP225W, AP325, AP327X
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2024-00012

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-45229, CVE-2023-45230, CVE-2023-45231, CVE-2023-45232, CVE-2023-45233, CVE-2023-45234, CVE-2023-45235, CVE-2023-38575, CVE-2023-39368, CVE-2024-0162, CVE-2024-0163, CVE-2023-29499, CVE-2023-48795)
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	PowerScale Archive A300 PowerScale Node Firmware Package - Versions prior to 12.2 PowerScale Archive A3000 PowerScale Node Firmware Package - Versions prior to 12.2 PowerScale Hybrid H700 PowerScale Node Firmware Package - Versions prior to 12.2 PowerScale Hybrid H7000 PowerScale Node Firmware Package - Versions prior to 12.2 PowerScale F200 PowerScale Node Firmware Package - Versions prior to 12.2 PowerScale F600 PowerScale Node Firmware Package - Versions prior to 12.2 PowerScale F900 PowerScale Node Firmware Package - Versions prior to 12.2 PowerScale B100 PowerScale Node Firmware Package - Versions prior to 12.2 PowerScale P100 PowerScale Node Firmware Package - Versions prior to 12.2 PowerScale F210 PowerScale Node Firmware Package - Versions prior to 12.2 PowerScale F710 PowerScale Node Firmware Package - Versions prior to 12.2 PowerScale F910 PowerScale Node Firmware Package - Versions prior to 12.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000226574/dsa-2024-267-security-update-for-dell-powerscale-onefs-for-multiple-security-vulnerabilities

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-35153, CVE-2022-42896, CVE-2023-1281, CVE-2023-1829, CVE-2023-2124, CVE-2023-2194, CVE-2023-2235, CVE-2023-26604, CVE-2023-2002, CVE-2023-3090, CVE-2023-3390, CVE-2023-3776, CVE-2023-4004, CVE-2023-20593, CVE-2023-35001, CVE-2023-35788, CVE-2024-27268, CVE-2024-22329, CVE-2024-25026, CVE-2024-22354, CVE-2024-22353, CVE-2023-51775, CVE-2024-31919, CVE-2024-21085, CVE-2024-22201, CVE-2024-35156, CVE-2024-35155, CVE-2024-35116, CVE-2024-31912, CVE-2023-50312, CVE-2024-21634, CVE-2023-38729, CVE-2012-2677, CVE-2024-25030, CVE-2024-25046, CVE-2024-27254, CVE-2023-52296, CVE-2024-22360, CVE-2023-48795, CVE-2023-45288, CVE-2024-25031, CVE-2024-38322, CVE-2024-33883)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Use After Free, Out of Bounds Access, Arbitrary Code Execution, Denial of Service. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	WebSphere Service Registry and Repository - version 8.5 Total Storage Service Console (TSSC) / TS4500 IMC - 9.4.14, 9.4.21, 9.4.26, 9.5.8 PowerVM Novalink - 2.0.0.0, 2.0.1, 2.0.2, 2.0.2.1, 2.0.3, 2.0.3.1, 2.1.0, 2.1.1, 2.2.0, 2.2.1 IBM WebSphere Remote Server - version 9.1, 9.0 IBM Storage Protect Server - versions from 8.1.0.000 to 8.1.22.xxx IBM Storage Protect Operations Center - versions from 8.1.0.000 to 8.1.22.xxx IBM Storage Defender - Resiliency Service - version 2.0.0-2.0.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7159303 • https://www.ibm.com/support/pages/node/7159375 • https://www.ibm.com/support/pages/node/7159376 • https://www.ibm.com/support/pages/node/7159377 • https://www.ibm.com/support/pages/node/7159320 • https://www.ibm.com/support/pages/node/7159317 • https://www.ibm.com/support/pages/node/7159315 • https://www.ibm.com/support/pages/node/7157218 • https://www.ibm.com/support/pages/node/7159291 • https://www.ibm.com/support/pages/node/7159285 • https://www.ibm.com/support/pages/node/7158519 • https://www.ibm.com/support/pages/node/7158513 • https://www.ibm.com/support/pages/node/7158516 • https://www.ibm.com/support/pages/node/7158446

Affected Product	**Cisco**
Severity	**Medium**
Affected Vulnerability	Command Injection Vulnerability (CVE-2024-20399)
Description	Cisco has released security updates addressing a Command Injection Vulnerability that exists in Cisco NX-OS Software. This Vulnerability could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Following Cisco products if they were running a vulnerable release of Cisco NX-OS* Software: • MDS 9000 Series Multilayer Switches • Nexus 3000 Series Switches • Nexus 5500 Platform Switches • Nexus 5600 Platform Switches • Nexus 6000 Series Switches • Nexus 7000 Series Switches • Nexus 9000 Series Switches in standalone NX-OS mode Nexus 3000 platforms: • N3K-C3264C-E • N3K-C3172PQ-10GE • N3K-C3172PQ-10GE-XL • N3K-C3172TQ-10GT • N3K-C3548P-10GX *Cisco NX-OS Software (Use Cisco Software Checker to identify vulnerable version)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP

Affected Product	**Dell**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-28972, CVE-2024-37126, CVE-2024-37134, CVE-2024-37133, CVE-2024-37132, CVE-2024-32854, CVE-2024-32852, CVE-2024-32853)
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	InsightIQ - Version 5.0 PowerScale OneFS - Version 8.2.2.x through 9.7.0.0 PowerScale OneFS - Version 9.7.0.1 through 9.7.0.2 PowerScale OneFS - Version 9.7.0.3 PowerScale OneFS - Version 9.8.0.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000226567/dsa-2024-211-security-update-for-a-dell-insightiq-broken-or-risky-cryptographic-algorithm-vulnerability • https://www.dell.com/support/kbdoc/en-us/000226569/dsa-2024-255-security-update-for-dell-powerscale-onefs-for-multiple-security-vulnerabilities

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.