Advisory Alert

Alert Number: AAA20231205 **Date:** December 5, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Red Hat	**High**	Multiple Vulnerabilities
Sonicwall	**High**	Multiple Vulnerabilities
Dell	**High**	Denial of Service Vulnerability
Ivanti	**High**, Medium	Multiple Vulnerabilities
IBM	**High**, Medium	Multiple Vulnerabilities

Description

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-2976, CVE-2023-4503, CVE-2023-26048, CVE-2023-26049, CVE-2023-35887, CVE-2023-39410, CVE-2023-44487)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. Successful exploitation of these vulnerabilities could lead to out-of-memory error, distributed denial of service and information disclosure. Red Hat recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	JBoss Enterprise Application Platform 7.4 for RHEL 8 x86_64 JBoss Enterprise Application Platform 7.4 for RHEL 9 x86_64 JBoss Enterprise Application Platform Text-Only Advisories x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2023:7641 https://access.redhat.com/errata/RHSA-2023:7639 https://access.redhat.com/errata/RHSA-2023:7638

Affected Product	**Sonicwall**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-44221, CVE-2023-5970)
Description	Sonicwall has released a security update addressing OS Command Injection and MFA Bypass Vulnerabilities that exist in their products. **CVE-2023-44221** - Improper neutralization of special elements in the SMA100 SSL-VPN management interface allows a remote authenticated attacker with administrative privilege to inject arbitrary commands as a 'nobody' user, potentially leading to OS Command Injection Vulnerability. **CVE-2023-5970** - Improper authentication in the SMA100 SSL-VPN virtual office portal allows a remote authenticated attacker to create an identical external domain user, resulting in an MFA bypass. Sonicwall recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Sonicwall SSL-VPN SMA100 version 10.X
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0018

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Denial of Service Vulnerability (CVE-2023-39248)
Description	Dell has released security updates addressing a Denial of Service Vulnerability. **CVE-2023-39248** -Dell OS10 Networking Switches running 10.5.2.x and above contain an Uncontrolled Resource Consumption (Denial of Service) vulnerability when switches are configured with VLT and VRRP. A remote unauthenticated attacker could potentially exploit this vulnerability, leading to Denial of Service for actual network users Dell recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Dell EMC Networking MX5108n MX SmartFabric OS10 Versions prior to 10.5.4.10 Dell EMC Networking MX5108n MX SmartFabric OS10 Versions prior to 10.5.5.7 Dell EMC Networking MX9116n MX SmartFabric OS10 Versions prior to 10.5.4.10 Dell EMC Networking MX9116n MX SmartFabric OS10 Versions prior to 10.5.5.7 Dell Networking OS10 10.5.5.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000219958/dsa-2023-382-security-update-for-dell-networking-mx-series-switches-vulnerability https://www.dell.com/support/kbdoc/en-us/000220138/dsa-2023-278-dell-networking-os10-security-updates-for-uncontrolled-resource-consumption

Affected Product	**Ivanti**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities(CVE-2023-39339, CVE-2023-39340, CVE-2023-41719, CVE-2023-41720)
Description	Ivanti has released security updates addressing multiple vulnerabilities. Successful exploitation of these vulnerabilities could lead to Denial of Service, remote code execution and arbitrary file read. **CVE-2023-39339**- A vulnerability exists on all versions of Ivanti Policy Secure below 22.6R1 where an authenticated administrator can perform an arbitrary file read via a maliciously crafted web request. **CVE-2023-39340**- A vulnerability exists on all versions of Ivanti Connect Secure below 22.6R2 where an attacker can send a specific request which may lead to Denial of Service (DoS) of the appliance. **CVE-2023-41719** - A vulnerability exists on all versions of Ivanti Connect Secure below 22.6R2 where an attacker impersonating an administrator may craft a specific web request which may lead to remote code execution. **CVE-2023-41720** - A vulnerability exists on all versions of Ivanti Connect Secure below 22.6R2 where a local attacker with access to an Ivanti Connect Secure (ICS) appliance can escalate their privileges by exploiting a vulnerable installed application. This vulnerability allows the attacker to gain elevated execution privileges on the affected system. Ivanti recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	All versions of Ivanti Connect Secure below 22.6R2 All versions of Ivanti Policy Secure below 22.6R1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://forums.ivanti.com/s/article/Security-patch-release-Ivanti-Connect-Secure-22-6R2-and-22-6R2-1?language=en_US https://forums.ivanti.com/s/article/Security-patch-release-Ivanti-Policy-Secure-22-6R1?language=en_US

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities(CVE-2023-1370, CVE-2022-3171, CVE-2022-3509, CVE-2023-43642, CVE-2023-34462, CVE-2018-25032, CVE-2002-0059, CVE-2022-37434, CVE-2015-8383, CVE-2015-8381, CVE-2015-8386, CVE-2015-8388, CVE-2015-8385, CVE-2015-8387, CVE-2015-8391, CVE-2015-8390, CVE-2015-8393, CVE-2015-8395, CVE-2015-8394, CVE-2015-2328, CVE-2015-2327, CVE-2020-14155, CVE-2015-8392, CVE-2023-47701, CVE-2023-40687, CVE-2023-38727, CVE-2023-40692, CVE-2023-43020, CVE-2023-46167, CVE-2023-45178, CVE-2023-29258, CVE-2023-32731, CVE-2022-3510, CVE-2023-38003)
Description	IBM has released security updates addressing multiple vulnerabilities. Successful exploitation of these vulnerabilities could lead to Denial of Service, sensitive information disclosure, arbitrary code execution. IBM recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	IBM Db2 10.5.0.11 Client and Server IBM Db2 10.5.0.x Client and Server IBM Db2 11.1.4.7 Client and Server IBM Db2 11.1.4.x Client and Server IBM Db2 11.5.6 through 11.5.8 Server IBM Db2 11.5.x Client and Server
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7087234 https://www.ibm.com/support/pages/node/7087162 https://www.ibm.com/support/pages/node/7087225 https://www.ibm.com/support/pages/node/7087197 https://www.ibm.com/support/pages/node/7087149 https://www.ibm.com/support/pages/node/7087143 https://www.ibm.com/support/pages/node/7087157 https://www.ibm.com/support/pages/node/7087180 https://www.ibm.com/support/pages/node/7087203 https://www.ibm.com/support/pages/node/7087207 https://www.ibm.com/support/pages/node/7087218 https://www.ibm.com/support/pages/node/7078681

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.