Advisory Alert

Alert Number: **AAA20231208** **Date:** **December 8, 2023**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**High**	Improper Privilege Management Security Vulnerability
F5	**High**	Denial of service vulnerability
Red Hat	**High**, **Medium**	Multiple Vulnerabilities
IBM	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Improper Privilege Management Security Vulnerability (CVE-2023-32460)
Description	Dell has released a security update addressing an Improper Privilege Management Security Vulnerability in Dell PowerEdge BIOS. An unauthenticated local attacker could potentially exploit this vulnerability, leading to privilege escalation. Dell recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Dell PowerEdge Dell EMC Storage NX3240 BIOS Versions prior to 2.20.1 Dell EMC Storage NX3340 BIOS Versions prior to 2.20.1 Dell EMC NX440 BIOS Versions prior to 2.15.1 Dell Storage NX3230 BIOS Versions prior to 2.18.1 Dell Storage NX3330 BIOS Versions prior to 2.18.1 Dell Storage NX430 BIOS Versions prior to 2.19.1 Dell XC Core Dell EMC XC Core Dell XC6320 Hyper-converged Appliance BIOS Versions prior to Before 2.18.2 Dell XC430 Hyper-converged Appliance BIOS Versions prior to Before 2.18.2 Dell XC630 Hyper-converged Appliance BIOS Versions prior to Before 2.18.1 Dell XC730 Hyper-converged Appliance BIOS Versions prior to Before 2.18.1 Dell XC730XD Hyper-converged Appliance BIOS Versions prior to Before 2.18.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000219550/dsa-2023-361-security-update-for-dell-poweredge-server-bios-for-an-improper-privilege-management-security-vulnerability

Affected Product	**F5**
Severity	**High**
Affected Vulnerability	Denial of service vulnerability (CVE-2022-41832)
Description	F5 has released a security update addressing a Denial of service vulnerability exists in all modules of BIG-IP products. **CVE-2022-41832-** Vulnerability in SIP profile configuration on a virtual server can lead to increased memory usage, causing system performance degradation. A remote attacker could exploit this, leading to denial-of-service. F5 recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	BIG-IP (all modules) 17.x 17.0.0 BIG-IP (all modules) 16.x 16.1.0 - 16.1.3 BIG-IP (all modules) 15.x 15.1.0 - 15.1.6 BIG-IP (all modules) 14.x 14.1.0 - 14.1.5 BIG-IP (all modules) 13.x 13.1.0 - 13.1.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K10347453

Affected Product	**Red Hat**
Severity	**High, Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2007-4559, CVE-2021-3826, CVE-2021-43618, CVE-2022-48468, CVE-2023-4016, CVE-2023-4641, CVE-2023-22745, CVE-2023-28321, CVE-2023-29491, CVE-2023-29499, CVE-2023-31486, CVE-2023-32611, CVE-2023-32665, CVE-2023-36054, CVE-2023-38545, CVE-2023-38546, CVE-2023-39325, CVE-2023-39975, CVE-2023-44487, CVE-2023-0464, CVE-2023-0465, CVE-2023-0466, CVE-2023-2650, CVE-2023-3446, CVE-2023-3817, CVE-2023-38039, CVE-2023-39615, CVE-2023-41081, CVE-2023-45802, CVE-2023-45853, CVE-2023-41080, CVE-2023-42794, CVE-2022-1471, CVE-2022-25857, CVE-2022-38749, CVE-2022-41854, CVE-2023-1370, CVE-2023-34050, CVE-2023-34462, CVE-2023-40167, CVE-2022-41724, CVE-2022-41725, CVE-2023-4586, CVE-2023-5384, CVE-2023-31582, CVE-2022-46751, CVE-2023-2976, CVE-2023-5072, CVE-2023-20873, CVE-2023-33201, CVE-2023-42445, CVE-2023-44387, CVE-2023-44981)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. Successful exploitation of these vulnerabilities could lead to heap based buffer overflow, Information Disclosure, Denial of service Red Hat recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	JBoss Enterprise Web Server 5 for RHEL 7 x86_64 JBoss Enterprise Web Server 5 for RHEL 8 x86_64 JBoss Enterprise Web Server 5 for RHEL 9 x86_64 JBoss Enterprise Web Server Text-Only Advisories x86_64 Red Hat Container Native Virtualization 4.14 for RHEL 7 x86_64 Red Hat Container Native Virtualization 4.14 for RHEL 8 x86_64 Red Hat Container Native Virtualization 4.14 for RHEL 9 x86_64 Red Hat Container Native Virtualization for ARM 64 4.14 for RHEL 8 aarch64 Red Hat Container Native Virtualization for ARM 64 4.14 for RHEL 9 aarch64 Red Hat JBoss AMQ Clients 3 for RHEL 8 x86_64 Red Hat JBoss AMQ Clients 3 for RHEL 9 x86_64 Red Hat JBoss Core Services 1 for RHEL 7 x86_64 Red Hat JBoss Core Services 1 for RHEL 8 x86_64 Red Hat JBoss Core Services Text-Only Advisories x86_64 Red Hat JBoss Data Grid Text-Only Advisories x86_64 Red Hat JBoss Middleware Text-Only Advisories for MIDDLEWARE 1 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2023:7622 https://access.redhat.com/errata/RHSA-2023:7623 https://access.redhat.com/errata/RHSA-2023:7625 https://access.redhat.com/errata/RHSA-2023:7626 https://access.redhat.com/errata/RHSA-2023:7672 https://access.redhat.com/errata/RHSA-2023:7676 https://access.redhat.com/errata/RHSA-2023:7678 https://access.redhat.com/errata/RHSA-2023:7697 https://access.redhat.com/errata/RHSA-2023:7704

Affected Product	**IBM**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-22081, CVE-2023-22067, CVE-2023-5676)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2023-22081**- An unspecified vulnerability in Oracle Java SE, Oracle GraalVM for JDK related to the JSSE component could allow a remote attacker to cause no confidentiality impact, no integrity impact, and low availability impact. **CVE-2023-22067**- An unspecified vulnerability in Oracle Java SE related to the CORBA component could allow a remote attacker to cause no confidentiality impact, low integrity impact, and no availability impact. **CVE-2023-5676-** Eclipse OpenJ9 is vulnerable to a denial of service, caused by a flaw when a shutdown signal (SIGTERM, SIGINT or SIGHUP) is received before the JVM has finished initializing. By sending a specially crafted request, a local authenticated attacker could exploit this vulnerability to cause an infinite busy hang on a spinlock or a segmentation fault. IBM recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	WebSphere Service Registry and Repository version 8.5.x WebSphere Service Registry and Repository Studio version 8.5.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7091183

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.