Advisory Alert

Alert Number: **AAA20230803** **Date:** **August 3, 2023**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
Suse	**Critical**	Multiple Vulnerabilities
Suse	**High**	Multiple Vulnerabilities
F5	**High, Medium**	Multiple Vulnerabilities
Cisco	**Medium**	Cross-Site Scripting Vulnerability
Qnap	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-29405, CVE-2023-29404, CVE-2023-29402, CVE-2023-29403)
Description	Dell has released a security update addressing multiple critical vulnerabilities that exist in third party components that affect Dell products. **CVE-2023-29405** - A flaw was found in golang. The go command may execute arbitrary code at build time when using cgo. This can be triggered by linker flags, specified via a "#cgo LDFLAGS" directive. The arguments for a number of flags which are non-optional are incorrectly considered optional, allowing disallowed flags to be smuggled through the LDFLAGS sanitization. This affects usage of both the gc and gccgo compilers. **CVE-2023-29404** - A flaw was found in golang. The go command may execute arbitrary code at build time when using cgo. This can be triggered by linker flags, specified via a "#cgo LDFLAGS" directive. Flags containing embedded spaces are mishandled, allowing disallowed flags to be smuggled through the LDFLAGS sanitization by including them in the argument of another flag. This only affects usage of the gccgo compiler. **CVE-2023-29402** - A flaw was found in golang. The go command may generate unexpected code at build time when using cgo. This may result in unexpected behavior when running a go program that uses cgo. This can occur when running an untrusted module that contains directories with newline characters in their names. **CVE-2023-29403** - On Unix platforms, the Go runtime does not behave differently when a binary is run with the setuid/setgid bits. This can be dangerous in certain cases, such as when dumping memory state or assuming the status of standard I/O file descriptors. Dell highly recommends applying necessary fixes to avoid issues
Affected Products	Dell Container Storage Modules Versions prior to 1.7.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000216414/dsa-2023-285-dell-container-storage-modules-security-update-for-multiple-vulnerabilities

Affected Product	**Suse**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-2183, CVE-2023-2801, CVE-2023-3128)
Description	Suse has released a security updates addressing multiple critical vulnerabilities affecting Suse manager 4.3.7 **CVE-2023-2183** - Grafana platform's option to send a test alert is not available from the user panel UI for users having the Viewer role. It is still possible for a user with the Viewer role to send a test alert using the API as the API does not check access to this function. This might enable malicious users to abuse the functionality by sending multiple alert messages to e-mail and Slack, spamming users, prepare Phishing attack or block SMTP server. **CVE-2023-2801** - Using public dashboards in Grafana, users can query multiple distinct data sources using mixed queries. However, such query has a possibility of crashing a Grafana instance. This might enable malicious users to crash Grafana instances through that endpoint. **CVE-2023-3128** - Grafana is validating Azure AD accounts based on the email claim. On Azure AD, the profile email field is not unique and can be easily modified. This leads to account takeover and authentication bypass when Azure AD OAuth is configured with a multi-tenant app. Suse highly recommends to apply the necessary security fixes at your earliest to avoid issues.
Affected Products	openSUSE Leap 15.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2023/suse-su-20233136-1

Affected Product	**Suse**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-2002, CVE-2023-2235, CVE-2023-33952, CVE-2023-35788)
Description	Suse has released a security updates addressing multiple vulnerabilities affecting their products. **CVE-2023-2002** - A vulnerability was found in the HCI sockets implementation due to a missing capability check in net/bluetooth/hci_sock.c in the Linux Kernel. This flaw allows an attacker to unauthorized execution of management commands, compromising the confidentiality, integrity, and availability of Bluetooth communication. **CVE-2023-2235** - A use-after-free vulnerability exsist in Linux Kernel Performance Events system that can be exploited to achieve local privilege escalation. **CVE-2023-33952** - A double-free vulnerability was found in the vmwgfx driver in the Linux kernel. The flaw exists within the handling of vmw_buffer_object objects. This flaw allows a local privileged user to escalate privileges and execute code in the context of the kernel. **CVE-2023-35788** - An issue was discovered in fl_set_geneve_opt in net/sched/cls_flower.c in the Linux kernel before 6.3.7. It allows an out-of-bounds write in the flower classifier code via TCA_FLOWER_KEY_ENC_OPTS_GENEVE packets. This may result in denial of service or privilege escalation. Suse recommends to apply the necessary security fixes at your earliest to avoid issues.
Affected Products	openSUSE Leap 15.5 SUSE Linux Enterprise High Performance Computing 15 SP5 SUSE Linux Enterprise Live Patching 15-SP5 SUSE Linux Enterprise Real Time 15 SP5 SUSE Linux Enterprise Server 15 SP5 SUSE Linux Enterprise Server for SAP Applications 15 SP5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2023/suse-su-20233153-1

Affected Product	**F5**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple vulnerabilities
Description	F5 has released a security update addressing multiple vulnerabilities affecting their products. If exploited these vulnerabilities could lead to Reflected cross-site scripting (XSS), Privilege escalation, Sensitive information disclosure, Modification of configured server list F5 recommends to apply the necessary security fixes at your earliest to avoid issues.
Affected Products	APM Clients 7.2.3 - 7.2.4 BIG-IP (all modules) 13.1.0 - 13.1.3, 14.1.0 - 14.1.5, 15.1.0 - 15.1.9, BIG-IP (all modules 16.1.0 - 16.1.3, 17.0.0 - 17.1.0 F5OS-A 1.4.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000135449 https://my.f5.com/manage/s/article/K000134922 https://my.f5.com/manage/s/article/K000134746 https://my.f5.com/manage/s/article/K000134535 https://my.f5.com/manage/s/article/K000133474 https://my.f5.com/manage/s/article/K000133472 https://my.f5.com/manage/s/article/K000132563

Affected Product	**Cisco**
Severity	**Medium**
Affected Vulnerability	Cross-Site Scripting Vulnerability (CVE-2023-20204)
Description	Cisco has released a security update addressing Cross-Site Scripting Vulnerability affecting their products. **CVE-2023-20204** - Cisco BroadWorks CommPilot Application Software's web-based management interface contains an Improper input Validation Vulnerability that could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. Cisco recommends to apply the necessary security fixes at your earliest to avoid issues.
Affected Products	Cisco BroadWorks Application Delivery Platform with CommPilot-25, CommPilot-24, and CommPilot-23 Release - Release Independent (RI). Cisco BroadWorks Application Server Software Release 23.0, 24.0 and Release Independent (RI). Cisco BroadWorks Xtended Services Platform Software Release 23.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-commpilot-xss-jC46sezF

Affected Product	**Qnap**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-32742, CVE-2022-2031, CVE-2022-32744, CVE-2022-32745, CVE-2022-32746)
Description	Qnap has released a security update addressing multiple vulnerabilities that exists in Samba that affect Qnap products. Exploitation of these vulnerabilities could lead to Sensitive information disclosure, Use-after-free condition, segmentation fault, Privilege Escalation. Qnap recommends to apply the necessary security fixes at your earliest to avoid issues.
Affected Products	QTS 5.0.1.2131 build prior to 20220820 QTS 5.0.0.2131 build prior to 20220815 QTS 4.5.4.2138 build prior to 20220824 QTS 4.3.6.2232 build prior to 20221124 QTS 4.3.4.2242 build prior to 20221124 QTS 4.3.3.2211 build prior to 20221124 QuTS hero h5.0.0.2120 build prior to 20220804 QuTS hero h4.5.4.2138 build prior to 20220824 QuTScloud prior to c5.0.1.2148
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.qnap.com/en-uk/security-advisory/qsa-22-22

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.