Advisory Alert

Alert Number: **AAA20240812** **Date:** **August 12, 2024**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Zabbix	**Critical**	Multiple Vulnerabilities
Dell	**High**	Arbitrary Code Execution Vulnerability
SUSE	**High**	Multiple Vulnerabilities
Cisco	**High**	RADIUS Protocol Spoofing Vulnerability
HPE	**High**	Arbitrary Code Execution Vulnerability
Qnap	**High**	Multiple Vulnerabilities
Redhat	**High**	Multiple Vulnerabilities
Zabbix	**High**, **Medium**, **Low**	Multiple Vulnerabilities

Description

Affected Product	**Zabbix**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-36461, CVE-2024-22116)
Description	Zabbix 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. **CVE-2024-36461**- Within Zabbix, users could directly modify memory pointers in the JavaScript engine. This vulnerability allows users with access to a single item configuration (limited role) to compromise the whole infrastructure of the monitoring solution by remote code execution. **CVE-2024-22116**- An administrator with restricted permissions can exploit the script execution functionality within the Monitoring Hosts section. The lack of default escaping for script parameters enabled this user ability to execute arbitrary code via the Ping script, thereby compromising infrastructure. Zabbix advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Zabbix Server version 6.0.0 - 6.0.30 Zabbix Server version 6.4.0 - 6.4.15 Zabbix Server version 7.0.0alpha1 - 7.0.0rc2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.zabbix.com/browse/ZBX-25018 • https://support.zabbix.com/browse/ZBX-25016

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Arbitrary Code Execution Vulnerability (CVE-2023-31315)
Description	Dell has released security updates addressing an Arbitrary Code Execution Vulnerability that exists in AMD third-party product that in turn affect Dell products. This vulnerability is caused due to improper validation in model specific register (MSR) which could allow a malicious program with ring0 access to modify SMM configuration while SMI lock is enabled. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	PowerEdge R6615 BIOS Versions prior to 1.8.3 PowerEdge R7615 BIOS Versions prior to 1.8.3 PowerEdge R6625 BIOS Versions prior to 1.8.3 PowerEdge R7625 BIOS Versions prior to 1.8.3 PowerEdge C6615 BIOS Versions prior to 1.3.3 PowerEdge R6515 BIOS Versions prior to 2.16.0 PowerEdge R6525 BIOS Versions prior to 2.16.2 PowerEdge R7515 BIOS Versions prior to 2.16.0 PowerEdge R7525 BIOS Versions prior to 2.16.2 PowerEdge C6525 BIOS Versions prior to 2.16.1 PowerEdge XE8545 BIOS Versions prior to 2.15.1 Dell EMC XC Core XC7525 BIOS Versions prior to 2.16.2 Dell XC Core XC7625 BIOS Versions prior to 1.8.3 PowerEdge R6415 BIOS Versions prior to 1.22.0 PowerEdge R7415 BIOS Versions prior to 1.22.0 PowerEdge R7425 BIOS Versions prior to 1.22.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000227665/dsa-2024-344-security-update-for-dell-amd-based-poweredge-server-vulnerabilities

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-26923, CVE-2024-27398, CVE-2024-35950)
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. 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 12 SP5, 15 SP4, 15 SP5 SUSE Linux Enterprise Live Patching 12 SP5, 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 12 SP5, 15 SP4, 15 SP5 SUSE Linux Enterprise Server for SAP Applications 12 SP512 SP5, 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-20242853-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20242827-1/

Affected Product	**Cisco**
Severity	**High**
Affected Vulnerability	RADIUS Protocol Spoofing Vulnerability (CVE-2024-3596)
Description	Cisco has released security updates addressing the RADIUS Protocol Spoofing Vulnerability that exists in their products. **CVE-2024-3596** - RADIUS Protocol under RFC 2865 is susceptible to forgery attacks by an on-path attacker who can modify any valid Response (Access-Accept, Access-Reject, or Access-Challenge) to any other response using a chosen-prefix collision attack against MD5 Response Authenticator signature. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	To find further details of the affected products please refer the Cisco Bug ID of the below mentioned products • Endpoint Clients and Client Software - Duo Authentication Proxy • Network and Content Security Devices ▪ Adaptive Security Appliance (ASA) ▪ Firepower Device Manager (FDM) ▪ Firepower Management Center (FMC) Software ▪ Firepower Threat Defense (FTD) Software ▪ Meraki MX Series Notes ▪ Identity Services Engine (ISE) ▪ Secure Email Gateway ▪ Secure Email and Web Manager ▪ Secure Firewall ▪ Secure Network Analytics ▪ Secure Web Appliance • Network Management and Provisioning ▪ Application Policy Infrastructure Controller (APIC) ▪ Crosswork Network Controller ▪ Nexus Dashboard, formerly Application Services Engine ▪ Prime Infrastructure • Routing and Switching - Enterprise and Service Provider ▪ ASR 5000 Series Routers ▪ Catalyst Center ▪ Catalyst SD-WAN Controller, formerly SD-WAN vSmart ▪ Catalyst SD-WAN Manager, formerly SD-WAN vManage ▪ Catalyst SD-WAN Validator, formerly SD-WAN vBond ▪ GGSN Gateway GPRS Support Node ▪ IOS Software ▪ IOS XE Software ▪ IOS XR Software ▪ IOx Fog Director ▪ MDS 9000 Series Multilayer Switches ▪ Nexus 1000V Series Switches ▪ Nexus 3000 Series Switches ▪ Nexus 5500 Platform Switches ▪ Nexus 5600 Platform Switches ▪ Nexus 6000 Series Switches ▪ Nexus 7000 Series Switches ▪ Nexus 9000 Series Fabric Switches in ACI Mode ▪ Nexus 9000 Series Switches in standalone NX-OS mode ▪ PGW Packet Data Network Gateway ▪ SD-WAN vEdge Routers ▪ System Architecture Evolution (SAE) Gateway ▪ Ultra Packet Core • Unified Computing ▪ Enterprise NFV Infrastructure Software (NFVIS) ▪ UCS Central Software ▪ UCS Manager • WirelessUnified Computing - AireOS Wireless LAN Controllers
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-radius-spoofing-july-2024-87cCDwZ3

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	Arbitrary Code Execution Vulnerability (CVE-2023-31315)
Description	HPE has released security updates addressing an Arbitrary Code Execution Vulnerability that exists in HPE ProLiant AMD Servers which could be locally exploited. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE ProLiant DL325 Gen11 Server - Prior to v1.64_06-19-2024 HPE ProLiant DL345 Gen11 Server - Prior to v1.64_06-19-2024 HPE ProLiant DL365 Gen11 Server - Prior to v1.64_06-19-2024 HPE ProLiant DL385 Gen11 Server - Prior to v1.64_06-19-2024 HPE ProLiant DL325 Gen10 Plus v2 server - Prior to v3.10_05-16-2024 HPE ProLiant DL345 Gen10 Plus server - Prior to v3.10_05-16-2024 HPE ProLiant DL365 Gen10 Plus server - Prior to v3.10_05-16-2024 HPE ProLiant DL385 Gen10 Plus server - Prior to v3.10_05-16-2024 HPE ProLiant DL385 Gen10 Plus v2 server - Prior to v3.10_05-16-2024 HPE ProLiant XL225n Gen10 Plus 1U Node - Prior to v3.10_05-16-2024 HPE ProLiant DL325 Gen10 Plus server - Prior to v3.10_05-16-2024 HPE ProLiant DL325 Gen10 Server - Prior to v3.10_05-16-2024 HPE ProLiant DL385 Gen10 Server - Prior to v3.10_05-16-2024
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04676en_us&docLocale=en_US

Affected Product	**Qnap**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-51364, CVE-2023-51365, CVE-2024-32765)
Description	Qnap has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2023-51364, CVE-2023-51365** - If exploited, the path traversal vulnerabilities could allow remote attackers to read sensitive data **CVE-2024-32765** - If exploited, the vulnerability could allow attackers to gain access to the system and execute certain functions. Qnap advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	QTS 5.1.x QTS 4.5.x QuTS hero h5.1.x QuTS hero h4.5.x QuTScloud c5.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.qnap.com/en/security-advisory/qsa-24-14

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-3653, CVE-2024-5971, CVE-2024-27316, CVE-2024-29025, CVE-2024-29857, CVE-2024-30171, CVE-2024-30172)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to system compromisation. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	JBoss Enterprise Application Platform 7.4 for RHEL 7 x86_64 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-2024:5143 • https://access.redhat.com/errata/RHSA-2024:5144 • https://access.redhat.com/errata/RHSA-2024:5145 • https://access.redhat.com/errata/RHSA-2024:5147

Affected Product	**Zabbix**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-22121, CVE-2024-22122, CVE-2024-22123, CVE-2024-22114, CVE-2024-36460, CVE-2024-36462)
Description	Zabbix has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to Remote Code Inclusion, Server Side Request Forgery, Retrieval of Embedded Sensitive Data, HTTP DoS. Zabbix advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Zabbix Agent, Server, Frontend versions • 5.0.0 - 5.0.42 • 6.0.0 - 6.0.30 • 6.4.0 - 6.4.15 • 7.0.0alpha1 - 7.0.0rc2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.zabbix.com/browse/ZBX-25011 • https://support.zabbix.com/browse/ZBX-25012 • https://support.zabbix.com/browse/ZBX-25013 • https://support.zabbix.com/browse/ZBX-25015 • https://support.zabbix.com/browse/ZBX-25017 • https://support.zabbix.com/browse/ZBX-25019

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.