Advisory Alert

Alert Number: AAA20240905 **Date:** September 5, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Veeam	**Critical**	Multiple Vulnerabilities
Cisco	**Critical**	Multiple Vulnerabilities
Veeam	**High**	Multiple Vulnerabilities
Netapp	**High**	Improper Input Validation Vulnerability
Dell	**High**	Multiple Vulnerabilities
Drupal	**High**, Medium	Multiple Vulnerabilities
Cisco	**High**, Medium	Multiple Vulnerabilities
Zimbra	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Veeam**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-40711, CVE-2024-42024, CVE-2024-42019, CVE-2024-38650, CVE-2024-39714)
Description	Veeam has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Remote Code Execution, Privilege Escalation, Arbitrary Code Execution. Veeam advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Veeam Backup & Replication 12.1.2.172 and all earlier version 12 builds. Veeam ONE 12.1.0.3208 and all earlier version 12 builds. Veeam Service Provider Console 8.1.0.21377 and all earlier version 8 builds.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.veeam.com/kb4649

Affected Product	**Cisco**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-20439, CVE-2024-20440)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in exist in their products. **CVE-2024-20439 -** A vulnerability in Cisco Smart Licensing Utility could allow an unauthenticated, remote attacker to log in to an affected system by using a static administrative credential. **CVE-2024-20440 -** A vulnerability in Cisco Smart Licensing Utility could allow an unauthenticated, remote attacker to access sensitive information. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Cisco Smart License Utility Release - 2.0.0, 2.1.0, 2.2.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cslu-7gHMzWmw#fs

Affected Product	**Veeam**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-40713, CVE-2024-40710, CVE-2024-39718, CVE-2024-40714, CVE-2024-40712, CVE-2024-40709, CVE-2024-42023, CVE-2024-42021, CVE-2024-42022, CVE-2024-42020, CVE-2024-39715, CVE-2024-38651, CVE-2024-40718)
Description	Veeam has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Remote Code Execution, Privilege Escalation, Arbitrary File Uploads. Veeam advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Veeam Backup & Replication 12.1.2.172 and all earlier version 12 builds. Veeam ONE 12.1.0.3208 and all earlier version 12 builds. Veeam Service Provider Console 8.1.0.21377 and all earlier version 8 builds. Veeam Agent for Linux 6.1.2.1781 and all earlier version 6 builds. Veeam Backup for Nutanix AHV Plug-In 12.5.1.8 and all earlier verion 12 builds. Veeam Backup for Oracle Linux Virtualization Manager and Red Hat Virtualization Plug-In 12.4.1.45 and all earlier version 12 builds.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.veeam.com/kb4649

Affected Product	**Netapp**
Severity	**High**
Affected Vulnerability	Improper Input Validation Vulnerability (CVE-2024-32007)
Description	NetApp has released security updates addressing an Improper Input Validation Vulnerability that exist in Apache products that in turn affect NetApp products. If exploited, it could lead to a Denial of Service (DoS). Netapp advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Snap Creator Framework
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.netapp.com/advisory/ntap-20240808-0009/

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-31102, CVE-2023-40481)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in 7-Zip products that in turn affect Dell products. **CVE-2023-31102** - Ppmd7.c in 7-Zip before 23.00 allows an integer underflow and invalid read operation via a crafted 7Z archive. **CVE-2023-40481 -** 7-Zip SquashFS File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of 7-Zip. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	iDRAC Service Module (Windows) - 7-Zip - Versions 5.2.0.0, 5.3.0.0, and 5.3.1.0 iDRAC Service Module (Linux) - 7-Zip - Versions 5.2.0.0, 5.3.0.0, and 5.3.1.0 iDRAC Service Module (VIB) for ESXi 7.0 U3 - 7-Zip - Versions 5.2.0.0, 5.3.0.0, and 5.3.1.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000228289/dsa-2024-379-security-update-for-dell-idrac-service-module-7-zip-vulnerability

Affected Product	**Drupal**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities
Description	Drupal has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Information Disclosure, Denial of Service, Cross Site Scripting. Drupal advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.drupal.org/sa-contrib-2024-038 • https://www.drupal.org/sa-contrib-2024-037 • https://www.drupal.org/sa-contrib-2024-036 • https://www.drupal.org/sa-contrib-2024-035 • https://www.drupal.org/sa-contrib-2024-034

Affected Product	**Cisco**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-20430, CVE-2024-20469, CVE-2024-20497, CVE-2024-20503, CVE-2021-1245, CVE-2021-1246)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Privilege Escalation, Command Injection, Information Disclosure, Cross-site Scripting. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Cisco Meraki SM Agent for Windows Release Prior to 4.2.0 Cisco Finesse releases earlier than Release 12.0(1) ES3 and Release 12.5(1) Cisco Virtualized Voice Browser releases after Release 12.6(1) Cisco Unified CVP release 12.6(2) ES4 through 12.6(2) ES17 Cisco Duo Epic for Hyperdrive Release - 1.0 Cisco Expressway-E Release - 14 and earlier, 15 Cisco ISE Release - 3.1 and earlier, 3.2, 3.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-agent-dll-hj-Ptn7PtKe • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-injection-6kn9tSxm • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expressway-auth-kdFrcZ2j • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-duo-epic-info-sdLv6h8y • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-multi-vuln-finesse-qp6gbUO2

Affected Product	**Zimbra**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-45513, CVE-2024-45519, CVE-2024-45518, CVE-2024-45194, CVE-2024-45517, CVE-2024-45515, CVE-2024-45516, CVE-2024-45514, CVE-2024-45511, CVE-2024-45512, CVE-2024-45510, CVE-2024-38356, CVE-2023-4863)
Description	Zimbra has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited to cause denial of service, security restriction bypass. Zimbra advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Zimbra Daffodil Versions Prior to 10.1.1 and 10.1.0 GA Zimbra Collaboration Daffodil Version Prior to 10.0.9 Zimbra Collaboration Kepler Version Prior to 9.0.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://wiki.zimbra.com/wiki/Zimbra_Releases/10.1.1#Security_Fixes • https://wiki.zimbra.com/wiki/Zimbra_Releases/10.0.9#Security_Fixes • https://wiki.zimbra.com/wiki/Zimbra_Releases/9.0.0/P41#Security_Fixes • https://wiki.zimbra.com/wiki/Zimbra_Releases/10.1.0#Security_Fixes

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.