Advisory Alert

Alert Number: AAA20240730 **Date:** July 30, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Commvault	**Critical**	Security Regression
ManageEngine	**High**	SQL Injection Vulnerability
Ubuntu	**High**, **Medium**, **Low**	Multiple Vulnerabilities
F5	**Medium**	Out-of-bounds Read Vulnerability
Red Hat	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Commvault**
Severity	**Critical**
Affected Vulnerability	Security Regression (CVE-2024-6387)
Description	Commvault has released security updates addressing a Security Regression in OpenSSH that affects Commvault Virtual Appliances (OVA) for Access Node and MediaAgent (FREL). **CVE-2024-6387** - A security regression (CVE-2006-5051) was discovered in OpenSSH's server (sshd). There is a race condition which can lead to sshd to handle some signals in an unsafe manner. An unauthenticated, remote attacker may be able to trigger it by failing to authenticate within a set time period. Commvault advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Commvault Virtual Appliances (OVA) for Access Node and MediaAgent (FREL).
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://documentation.commvault.com/securityadvisories/CV_2024_07_1.html#impacted-products

Affected Product	**ManageEngine**
Severity	**High**
Affected Vulnerability	SQL Injection Vulnerability (CVE-2024-6748)
Description	ManageEngine has released security updates addressing an SQL Injection Vulnerability that exists in their products. Using this SQL injection, it is possible to execute custom queries and access the database table entries. ManageEngine advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	OpManager Versions 128317 and prior OpManager Plus Versions 128317 and prior OpManager MSP Versions 128317 and prior RMM Versions 128317 and prior
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.manageengine.com/itom/advisory/cve-2024-6748.html

Affected Product	**Ubuntu**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-26882, CVE-2024-24858, CVE-2024-24859, CVE-2024-36902, CVE-2024-26840, CVE-2024-26857, CVE-2024-25739, CVE-2024-26886, CVE-2023-52752, CVE-2024-36016, CVE-2024-26901, CVE-2023-52469, CVE-2023-52449, CVE-2024-35997, CVE-2024-27020, CVE-2023-52436, CVE-2024-26923, CVE-2024-26934, CVE-2023-52435, CVE-2023-52443, CVE-2024-35978, CVE-2024-35984, CVE-2024-25744, CVE-2024-27013, CVE-2024-26884, CVE-2023-46343, CVE-2023-52444, CVE-2024-35982, CVE-2024-24857, CVE-2023-52620, CVE-2024-26583, CVE-2022-48655, CVE-2024-26585, CVE-2024-26584, CVE-2021-47131, CVE-2024-26907, CVE-2024-35992, CVE-2024-25742, CVE-2024-36008, CVE-2024-35990, CVE-2024-27017, CVE-2024-26952)
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Arbitrary Code Execution, Denial of Service, Information Disclosure. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 14.04 Ubuntu 20.04 Ubuntu 16.04 Ubuntu 22.04 Ubuntu 18.04 Ubuntu 24.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://ubuntu.com/security/notices/USN-6926-1 • https://ubuntu.com/security/notices/USN-6925-1 • https://ubuntu.com/security/notices/USN-6924-1 • https://ubuntu.com/security/notices/USN-6923-1 • https://ubuntu.com/security/notices/USN-6922-1 • https://ubuntu.com/security/notices/USN-6921-1

Affected Product	**F5**
Severity	**Medium**
Affected Vulnerability	Out-of-bounds Read Vulnerability (CVE-2022-28615)
Description	F5 has released security updates addressing an Out-of-bounds Read Vulnerability that exists in BIG-IP systems. **CVE-2022-28615** - Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	BIG-IP (all modules) versions: • 17.x Branch - 17.0.0 - 17.1.0 • 16.x Branch - 16.1.0 - 16.1.3 • 15.x Branch - 15.1.0 - 15.1.8
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K40582331

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-47548, CVE-2022-48743, CVE-2023-52667, CVE-2023-52784, CVE-2024-26733, CVE-2024-26852, CVE-2024-26908, CVE-2024-35960, CVE-2024-36020, CVE-2024-36025, CVE-2024-36924, CVE-2024-36929, CVE-2024-38596)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in Red Hat Enterprise Linux kernel. These vulnerabilities could be exploited by malicious users to compromise the affected system. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat Enterprise Linux Server - AUS 8.6 x86_64 Red Hat Enterprise Linux Server - TUS 8.6 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.6 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.6 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2024:4902

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.