Advisory Alert

Alert Number: AAA20240718 **Date:** July 18, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**Critical**	Multiple Vulnerabilities
Oracle	**Critical**	Multiple Vulnerabilities
Apache HTTP Server	**High**	Multiple Vulnerabilities
Ivanti	**High**, Medium	Multiple Vulnerabilities
IBM	**High**, Medium	Multiple Vulnerabilities
Cisco	**High**, Medium	Multiple Vulnerabilities
Ubuntu	**High**, Medium, Low	Multiple Vulnerabilities

Description

Affected Product	**Cisco**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-20419, CVE-2024-20401)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2024-20419 -** A vulnerability in the authentication system of Cisco Smart Software Manager On-Prem (SSM On-Prem) could allow an unauthenticated, remote attacker to change the password of any user, including administrative users. **CVE-2024-20401 -** A vulnerability in the content scanning and message filtering features of Cisco Secure Email Gateway could allow an unauthenticated, remote attacker to overwrite arbitrary files on the underlying operating system. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Cisco AsyncOS and both of the following conditions are met: • Either the file analysis feature, which is part of Cisco Advanced Malware Protection (AMP), or the content filter feature is enabled and assigned to an incoming mail policy • The Content Scanner Tools version is earlier than 23.3.0.4823 Cisco SSM On-Prem Release 8-202206 and earlier
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cssm-auth-sLw3uhUy • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-afw-bGG2UsjH

Affected Product	**Oracle**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Oracle has released July 2024 Security Updates addressing multiple vulnerabilities that exist in Oracle Linux, Oracle Solaris, Oracle VM Server and Third Party components used in Oracle products. These vulnerabilities could be exploited by malicious users to compromise the affected system. Oracle 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.oracle.com/security-alerts/cpujul2024.html • https://www.oracle.com/security-alerts/bulletinjul2024.html • https://www.oracle.com/security-alerts/linuxbulletinjul2024.html • https://www.oracle.com/security-alerts/ovmbulletinjul2024.html

Affected Product	**Apache HTTP Server**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-40725, CVE-2024-40898)
Description	Apache has released security updates addressing multiple vulnerabilities that exist in their Apache HTTP Server. **CVE-2024-40725 -** A partial fix for CVE-2024-39884 in the core of Apache HTTP Server 2.4.61 ignores some use of the legacy content-type based configuration of handlers. "AddType" and similar configuration, under some circumstances where files are requested indirectly, result in source code disclosure of local content. For example, PHP scripts may be served instead of interpreted. **CVE-2024-40898 -** SSRF in Apache HTTP Server on Windows with mod_rewrite in server/vhost context, allows to potentially leak NTML hashes to a malicious server via SSRF and malicious requests. Apache advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Apache 2.4.0 through 2.4.61
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://httpd.apache.org/security/vulnerabilities_24.html

Affected Product	**Ivanti**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-36130, CVE-2024-36131, CVE-2024-36132, CVE-2024-34788)
Description	Ivanti has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could allow malicious users to Execute Arbitrary codes, Bypass Authentication, Access Sensitive Information. Ivanti advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ivanti Endpoint Manager for Mobile Prior to 12.1.0.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-for-Mobile-EPMM-July-2024?language=en_US

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-20952, CVE-2024-20945, CVE-2024-20918, CVE-2024-20921, CVE-2024-20926, CVE-2024-20919)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may compromise the affected system. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Storage Scale System - Versions 6.1.0.0 - 6.1.9.2 IBM Elastic Storage Server - Versions 6.1.0.0 - 6.1.9.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7160487 • https://www.ibm.com/support/pages/node/7160488

Affected Product	**Cisco**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-20296, CVE-2024-20323, CVE-2024-20395, CVE-2024-20396, CVE-2024-20400, CVE-2024-20416, CVE-2024-20429, CVE-2024-20435)
Description	Cisco has released security updates addressing multiple vulnerabilities that exists in their products. These vulnerabilities could be exploited by malicious users to cause Arbitrary code Execution, Denial of Service, Privilege escalation, Web Page Redirection. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Cisco Small Business Router Firmware Release 1.0.03.24 or later: • RV340 Dual WAN Gigabit VPN Routers • RV340W Dual WAN Gigabit Wireless-AC VPN Routers • RV345 Dual WAN Gigabit VPN Routers • RV345P Dual WAN Gigabit PoE VPN Routers Cisco AsyncOS for Secure Email Gateway Release 14.2 and earlier, 15.0 Cisco Expressway Series Release 15 and Earlier Cisco Webex App and were addressed through the Cisco Webex service Cisco iNode Software Release 3.1.2 and earlier Cisco iNode Manager Software Release 23.1 and earlier Cisco ISE Release 3.1, 3.2, 3.3, 3.0 and earlier Cisco AsyncOS for Secure Web Appliance Release 15.0, 15.1, 15.2, 14.5 and Earlier
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-priv-esc-ssti-xNO2EOGZ • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expressway-redirect-KJsFuXgj • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv34x-rce-7pqFU2e • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-app-ZjNm8X8j • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-inode-static-key-VUVCeynn • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-file-upload-krW2TxA9 • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-swa-priv-esc-7uHpZsCC

Affected Product	**Ubuntu**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
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, NULL Pointer Dereference, Integer Overflow. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 20.04 Ubuntu 22.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://ubuntu.com/security/notices/USN-6900-1 • https://ubuntu.com/security/notices/USN-6896-3

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.