Advisory Alert

Alert Number: AAA20220407 **Date:** April 7, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Vmware	**Critical**	Multiple Vulnerabilities
Cisco	**Medium**	Multiple Vulnerabilities

Description

Affected Product	Vmware
Severity	**Critical**
Affected Vulnerability	Multiple vulnerabilities (CVE-2022-22962, CVE-2022-22964, CVE-2022-22954, CVE-2022-22955, CVE-2022-22956, CVE-2022-22957, CVE-2022-22958, CVE-2022-22959, CVE-2022-22960, CVE-2022-22961)
Description	VMware has released Security Updates addressing multiple vulnerabilities including privilege escalation, Server-side Template Injection Remote Code Execution, Authentication Bypass, JDBC Injection Remote Code Execution, Cross Site Request Forgery and Information Disclosure vulnerability that contains in their products which leads attackers to perform malicious activities. VMware highly recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	VMware Workspace ONE Access (Access) VMware Identity Manager (vIDM) VMware vRealize Automation (vRA) VMware Cloud Foundation vRealize Suite Lifecycle Manage VMware Horizon Client for Linux
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.vmware.com/security/advisories/VMSA-2022-0012.html https://www.vmware.com/security/advisories/VMSA-2022-0011.html

Affected Product	Cisco
Severity	**Medium**
Affected Vulnerability	Multiple vulnerabilities (CVE-2022-20675, CVE-2022-20782, CVE-2022-20741, CVE-2022-20784, CVE-2022-20774, CVE-2022-20763, CVE-2022-20781)
Description	Cisco has released security updates addressing multiple vulnerabilities which may lead attackers to cause stored cross-site scripting (XSS) attack, arbitrary code injection, cross-site request forgery (CSRF) attack, bypass established web request policies and access blocked content, sensitive data disclosure and denial of service conditions. Cisco highly recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	Cisco WSA, both virtual and hardware versions Cisco Webex Meetings (cloud based) IP Phone 6800 Series with Multiplatform Firmware IP Phone 7800 Series with Multiplatform Firmware IP Phone 8800 Series with Multiplatform Firmware Network Diagrams application of Cisco Secure Network Analytics Cisco ISE Cisco AsyncOS Software ESA, Secure Email and Web Manager
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wsa-stored-xss-XPsJghMY https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-java-MVX6crH9 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-voip-phone-csrf-K56vXvVx https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sna-xss-mCA9tQnJ https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-swa-filter-bypass-XXXTU3X https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-info-exp-YXAWYP3s https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ESA-SNMP-JLAJksWK

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.