Advisory Alert

Alert Number: AAA20220803 **Date:** August 3, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
VMware	**Critical**	Authentication Bypass Vulnerability
Cisco	**Critical**	Authentication Bypass Vulnerability
VMware	**High**, **Medium**	Multiple Vulnerabilities
RedHat	**High**, **Medium**	Multiple Vulnerabilities
FortiGate	**High**, **Medium**	Multiple Vulnerabilities

Description

Affected Product	**VMware**
Severity	**Critical**
Affected Vulnerability	Authentication Bypass Vulnerability (CVE-2022-31656)
Description	VMware has released a patch update addressing a critical authentication bypass vulnerability that exists in their products. Using this vulnerability an attacker with network access to the UI may be able to obtain administrative access without the need to authenticate. 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)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.vmware.com/security/advisories/VMSA-2022-0021.html

Affected Product	**Cisco**
Severity	**Critical**
Affected Vulnerability	Authentication Bypass Vulnerability (CVE-2022-20798)
Description	Cisco has released a patch update addressing a critical External Authentication Bypass Vulnerability that exists in the Cisco Secure Email and Web Manager, formerly known as Cisco Security Management Appliance (SMA), and Cisco Email Security Appliance (ESA). This vulnerability exists because of improper authentication checks when an affected device uses Lightweight Directory Access Protocol (LDAP) for external authentication. An attacker can exploit this vulnerability by entering a specific input on the login page of the affected device. The exploitation of this vulnerability could allow the attacker to gain unauthorized access to the web-based management interface of the affected device. Cisco highly recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	Cisco Secure Email and Web Manager Cisco Email Security Appliance
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sma-esa-auth-bypass-66kEcxQD

Affected Product	**VMware**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-31657, CVE-2022-31658, CVE-2022-31659, CVE-2022-31660, CVE-2022-31661, CVE-2022-31662, CVE-2022-31663, CVE-2022-31664, CVE-2022-31665)
Description	VMware has released a patch update addressing multiple vulnerabilities that exists in their products including JDBC Injection Remote Code Execution, SQL injection Remote Code Execution, Local Privilege Escalation, URL Injection, Path traversal and Cross-site scripting (XSS). VMware highly recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	VMware Workspace ONE Access (Access) VMware Workspace ONE Access Connector (Access Connector) VMware Identity Manager (vIDM) VMware Identity Manager Connector (vIDM Connector) VMware vRealize Automation (vRA) VMware Cloud Foundation vRealize Suite Lifecycle Manager
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.vmware.com/security/advisories/VMSA-2022-0021.html

Affected Product	**RedHat**
Severity	**High, Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-1012, CVE-2022-32250, CVE-2021-4206, CVE-2021-4207, CVE-2022-26353, CVE-2022-26354)
Description	RedHat has released patch updates to address multiple flaws that exist in their products. The exploitation of these vulnerabilities could cause privilege escalation to root, information leakage, heap buffer overflow, map leaking on error during receive, memory leakage RedHat highly recommends to apply necessary fixes to avoid issues.
Affected Products	Red Hat Enterprise Linux for Real Time 8 x86_64 Red Hat Enterprise Linux for Real Time for NFV 8 x86_64 Red Hat Virtualization Host 4 for RHEL 8 x86_64 Red Hat Enterprise Linux for x86_64 8 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 8.6 x86_64 Red Hat Enterprise Linux Server - TUS 8.6 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.6 x86_64 Red Hat Enterprise Linux Server - AUS 8.6 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2022:5834 https://access.redhat.com/errata/RHSA-2022:5819 https://access.redhat.com/errata/RHSA-2022:5821 https://access.redhat.com/errata/RHSA-2022:5839

Affected Product	**FortiGate**	
Severity	**High, Medium**	
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-22299, CVE-2022-27484, CVE-2022-23442)	
Description	FortiGate has released security updates addressing multiple vulnerabilities that exists in their Products. The exploitation of these vulnerabilities could cause unauthorized code or commands execution, bypass old password check in the password change form and gather the checksum information about the other VDOMs via CLI commands. FortiGate recommends to apply necessary security fixes at earliest to avoid issues	
Affected Products	FortiOS version 7.0.0 through 7.0.5 FortiOS version 6.4.0 through 6.4.8 FortiOS version 6.2.0 through 6.2.11 FortiADC version 6.2.0 through 6.2.3 FortiADC version 6.1.0 through 6.1.6 FortiADC version 6.0.0 through 6.0.4 FortiADC version 5.4.0 through 5.4.5 FortiADC version 5.3.0 through 5.3.7 FortiADC version 5.2.0 through 5.2.8 FortiADC version 5.1.0 through 5.1.7 FortiADC version 5.0.0 through 5.0.4 FortiADC version 6.1.0 through 6.1.5	FortiADC version 6.2.0 through 6.2.1 FortiProxy version 1.0.0 through 1.0.7 FortiProxy version 1.1.0 through 1.1.6 FortiProxy version 1.2.0 through 1.2.13 FortiProxy version 2.0.0 through 2.0.7 FortiProxy version 7.0.0 through 7.0.1 FortiOS version 6.0.0 through 6.0.14 FortiOS version 6.2.0 through 6.2.10 FortiOS version 7.0.0 through 7.0.2 FortiMail version 6.4.0 through 6.4.5 FortiMail version 7.0.0 through 7.0.2
Officially Acknowledged by the Vendor	Yes	
Patch/ Workaround Released	Yes	
Reference	https://www.fortiguard.com/psirt/FG-IR-21-235 https://www.fortiguard.com/psirt/FG-IR-22-055 https://www.fortiguard.com/psirt/FG-IR-22-036	

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.