Advisory Alert

Alert Number: AAA20220519 **Date:** May 19, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
VMware	**Critical**	Multiple Vulnerabilities
Redhat	**High**	Multiple Vulnerabilities
Cisco	**Medium**	Multiple Vulnerabilities
Sonicwall	**Medium**	Remote Code execution

Description

Affected Product	VMware
Severity	**Critical**
Affected Vulnerability	Multiple vulnerabilities (CVE-2022-22972, CVE-2022-22973)
Description	VMware has released security updates addressing Multiple Vulnerabilities that exist in their products. **CVE-2022-22972**- VMware Workspace ONE Access, Identity Manager and vRealize Automation are affected with an authentication bypass vulnerability. Without the need to authenticate, a malicious actor with network access to the UI may be able to gain administrative access. **CVE-2022-22973**- VMware Workspace ONE Access and Identity Manager has a privilege escalation vulnerability. With local access, a malicious actor can elevate privileges to 'root.' VMware recommends applying necessary fixes 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
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.vmware.com/security/advisories/VMSA-2022-0014.html

Affected Product	Redhat
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-0492, CVE-2022-1271, CVE-2022-24070, CVE-2022-29909, CVE-2022-29911, CVE-2022-29914, CVE-2022-29916, CVE-2022-29917, CVE-2022-29912, CVE-2022-29913, CVE-2022-1520)
Description	Redhat has released security updates addressing multiple vulnerabilities that exists in their products. These vulnerabilities allow an attacker to cause arbitrary-file-write, memory corruption and permission prompt in nested browsing context bypass, privilege escalation. Redhat highly recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2022:4591 https://access.redhat.com/errata/RHSA-2022:4582 https://access.redhat.com/errata/RHSA-2022:4589 https://access.redhat.com/errata/RHSA-2022:4655 https://access.redhat.com/errata/RHSA-2022:4644 https://access.redhat.com/errata/RHSA-2022:4642

Affected Product	Cisco
Severity	**Medium**
Affected Vulnerability	Multiple vulnerabilities (CVE-2022-20797, CVE-2022-20806, CVE-2022-20807, CVE-2022-20809, CVE-2022-20802, CVE-2022-20666, CVE-2022-20667, CVE-2022-20668, CVE-2022-20765)
Description	Cisco has released security updates addressing multiple vulnerabilities that exists in their products. Successful exploitation of the vulnerabilities could cause remote code execution, arbitrary code execution, cross-site scripting. Cisco highly recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	Cisco Secure Network Analytics Earlier than 7.4.1 Cisco Expressway Series and Cisco TelePresence VCS Release 14.0 and earlier Cisco ECE Software Release Earlier than 12.6(1) ES2 Cisco CSPC Release 2.10, 2.9 and earlier Cisco UCS Director Release 6 and earlier
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-stealth-rce-2hYb9KFK https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expressway-filewrite-bsFVwueV https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ece-strd-xss-BqFXO9D2 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cspc-multi-xss-tyDFjhwb https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-UCS-XSS-uQSME3L7

Affected Product	Sonicwall
Severity	**Medium**
Affected Vulnerability	Remote Code execution (CVE-2022-1703)
Description	Soinwall has identified a remote code execution vulnerability impacting SMA100 series firmware. The SonicWall SSL-VPN SMA100 series management interface's improper neutralization of special elements allows a remote authenticated attacker to inject OS Command as the 'root' user, potentially leading to a remote command execution vulnerability or denial of service attack.
Affected Products	SMA100 series firmware 10.2.1.4-31sv and earlier versions. SMA100 series firmware 10.2.0.9-41sv and earlier versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0010

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.