Advisory Alert

Alert Number: AAA20211222 **Date:** December 22, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
VMware	**Critical**	Multiple Vulnerabilities
SonicWall	**High**	Multiple Vulnerabilities

Description

Affected Product	VMware
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-22054, CVE-2021-22048, CVE-2021-22056, CVE-2021-22057)
Description	VMware has released Security Updates addressing multiple vulnerabilities that exist with VMware products. **CVE-2021-22054 -** A malicious actor with network access to UEM can send their requests without authentication and may exploit this Server-Side Request Forgery (SSRF) vulnerability in VMware Workspace ONE UEM console to gain access to sensitive information. **CVE-2021-22048 -** A malicious actor with non-administrative access to vCenter Server may exploit this privilege escalation vulnerability in the VMware Center Server to elevate privileges to a higher privileged level. **CVE-2021-22056 -** VMware Workspace ONE Access and Identity Manager contain a Server-Side Request Forgery vulnerability, and malicious actor with network access may be able to make HTTP requests to arbitrary origins and read the full response. **CVE-2021-22057 -** A malicious actor, who has successfully provided first-factor authentication may be able to obtain second-factor authentication provided by VMware Verify by bypassing VMware Workspace ONE Access authentication.
Affected Products	VMware Workspace ONE UEM console VMware vCenter Server (vCenter Server) VMware Cloud Foundation (Cloud Foundation) VMware Workspace ONE Access (Access) VMware Identity Manager (vIDM) 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-2021-0029.html https://www.vmware.com/security/advisories/VMSA-2021-0025.html https://www.vmware.com/security/advisories/VMSA-2021-0030.html

Affected Product	**SonicWall**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-20047, CVE-2021-20049, CVE-2021-20050)
Description	SonicWall has released Security Updates addressing multiple vulnerabilities that exist with SonicWall products. **CVE-2021-20047 -** A local attacker can successfully exploit a DLL Search Order Hijacking vulnerability that exists in the SonicWall Global VPN client and it could result in remote code execution on the target system. **CVE-2021-20049 -** A remote unauthenticated attacker can perform SMA100 username enumeration based on the server responses by using a vulnerability in SonicWall SMA100 password update API. **CVE-2021-20050 -** Improper Access Control Vulnerability in the SMA100 series allowed to access restricted management APIs without a user login and expose configuration meta-data.
Affected Products	Global VPN Client (32-bit & 64-bit) version 4.10.6 (32-bit & 64-bit) & earlier SMA100 firmware 10.2.1.2-24sv and earlier SMA100 firmware 10.2.0.8-37sv and earlier
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0025 https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0030 https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0031

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.