Advisory Alert

Alert Number: AAA20211208 **Date:** December 8, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Fortinet	**Critical**	Multiple Vulnerabilities
SonicWall	**Critical**	Multiple Vulnerabilities

Description

Affected Product	**Fortinet**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-43065, CVE-2021-43068, CVE-2021-43067, CVE-2021-43204, CVE-2021-36167, CVE-2021-41030, CVE-2021-41028, CVE-2021-36189, CVE-2021-41021, CVE-2021-43065, CVE-2021-26103, CVE-2021-41024, CVE-2021-42757, CVE-2021-26108, CVE-2021-36173, CVE-2021-26109, CVE-2021-44168, CVE-2021-26110, CVE-2021-32591, CVE-2021-42758, CVE-2021-42760, CVE-2021-42752, CVE-2021-41029, CVE-2021-36190, CVE-2021-41017, CVE-2021-41014, CVE-2021-36195, CVE-2021-41025, CVE-2021-36180, CVE-2021-36191, CVE-2021-43064, CVE-2021-41026, CVE-2021-41015, CVE-2021-36188, CVE-2021-43063, CVE-2021-41027, CVE-2021-36194, CVE-2021-41013, CVE-2021-43071, CVE-2021-42759)
Description	Fortinet has released its Security Patch Updates for December 2021 to address 40 vulnerabilities across multiple products. An attacker could exploit some of these vulnerabilities to trigger Improper access control, command injection, sensitive information disclosure, denial of service, elevation of privilege, SQL injection, and cross-site scripting on the targeted system. Fortinet highly recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	FortiNAC FortiAuthenticator FortiClient (Windows) FortiClient EMS FortiOS FortiProxy FortiSandbox FortiWeb FortiADC FortiMail FortiWLC FortiWLM Meru AP
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt?date=12-2021

Affected Product	**SonicWall**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-20038, CVE-2021-20039, CVE-2021-20040, CVE-2021-20041, CVE-2021-20042, CVE-2021-20043, CVE-2021-20044, CVE-2021-20045)
Description	SonicWall has released Security Updates addressing multiple SMA100 affected vulnerabilities such as Unauthenticated Stack-Based Buffer Overflow vulnerability, Authenticated Command Injection vulnerability, Unauthenticated File Upload Path Traversal vulnerability, Unauthenticated CPU Exhaustion vulnerability, Unauthenticated Confused Deputy vulnerability, Heap-Based Buffer Overflow vulnerability, Post-Authentication Remote Command Execution vulnerability and Multiple Unauthenticated Heap-Based and Stack Based Buffer Overflow vulnerability. It is highly recommended to apply necessary fixes provided on the official SonicWall website at the earliest to avoid these security issues, and all SonicWall users are encouraged to upgrade to the latest versions.
Affected Products	SonicWall SMA 100 Series
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026

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.