Advisory Alert

Alert Number: AAA20221014 **Date:** October 14, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Pulse Secure	**High**, **Medium**	Multiple Denial of Service Vulnerabilities
SonicWall	**Medium**	Path Manipulation Vulnerability

Description

Affected Product	**Pulse Secure**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Denial of Service Vulnerabilities (CVE-2022-35254,CVE-2022-35258)
Description	Pulse Secure has released a security update addressing multiple denial of service vulnerabilities that exists in the Ivanti Connect Secure (ICS) product. Using these vulnerabilities an authenticated attacker can cause denial of service condition in the system. Pulse Secure highly recommends to apply the necessary patch updates at your earliest to avoid issues
Affected Products	Ivanti Connect Secure (ICS) versions prior to 9.1R14.3, 9.1R15.2, 9.1R16.2, and 22.2R4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA45520/?kA23Z000000GH5OSAW

Affected Product	**SonicWall**
Severity	**Medium**
Affected Vulnerability	Path Manipulation Vulnerability (CVE-2021-20030)
Description	SonicWall has released a security update addressing a path manipulation vulnerability that exists in the SonicWall GMS product. Using this vulnerability an unauthenticated attacker can gain access to web directory containing application's binaries and configuration files. SonicWall highly recommends to apply the necessary patch updates at your earliest to avoid issues
Affected Products	SonicWall GMS versions prior to version 9.3.2.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0021

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.