TLP: WHITE

Advisory Alert

Alert Number: **AAA20210505** **Date:** **May 5, 2021**

Document Classification Level : Public Circulation Permitted

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Pulse Secure	**Critical**	Multiple Vulnerabilities
Fortinet	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Pulse Secure**
Severity	**Critical**
Affected Vulnerability	Multiple vulnerabilities (CVE-2021-22893, CVE-2021-22894, CVE-2021-22899, CVE-2021-22900)
Description	Pulse Secure has released security updates addressing the critical Multiple vulnerability in Pulse Connect Secure. **CVE-2021-22893 -** Multiple use after free in PCS before 9.1R11.4 allows a remote unauthenticated attacker to execute arbitrary code via license server web services. **CVE-2021-22894 -** Buffer overflow in PCS Collaboration Suite before 9.1R11.4 allows a remote authenticated user to execute arbitrary code as the root user via maliciously crafted meeting room. **CVE-2021-22899 -** Command Injection in PCS before 9.1R11.4 allows a remote authenticated user to perform remote code execution via Windows File Resource Profiles. **CVE-2021-22900 -** Multiple unrestricted uploads in PCS before 9.1R11.4 allow an authenticated administrator to perform a file write via a maliciously crafted archive upload in the administrator web interface.
Affected Products	Prior to update Pulse Connect Secure 9.1R11.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44784/

Affected Product	**Fortinet**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-24011, CVE-2019-15706, CVE-2021-22126, CVE-2021-24023)
Description	Fortinet has released security updates addressing the critical Multiple vulnerability in their products. CVE-2021-24011 - A privilege escalation vulnerability in FortiNAC may allow an admin user to escalate the privileges to root by abusing the sudo privileges. CVE-2019-15706 - An improper neutralization of input during web page generation in the SSL VPN portal of FortiProxy may allow a remote authenticated attacker to perform a stored cross site scripting attack. CVE-2021-22126 - A use of hard-coded password vulnerability in Meru AP may allow a remote authenticated attacker to access the system as root using the default hard-coded username and password. CVE-2021-24023 - An improper input validation in FortiAI v1.4.0 may allow an authenticated user to gain system shell access via a malicious payload in the "diagnose" command.
Affected Products	FortiNAC version 8.8.1 and below. FortiProxy version 2.0.0. FortiProxy versions 1.2.9 and below. Meru AP versions 8.5.2 and below. Any FortiAI firmware less than or equal to v1.4.0 is impacted.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-20-038 https://www.fortiguard.com/psirt/FG-IR-20-226 https://www.fortiguard.com/psirt/FG-IR-20-147 https://www.fortiguard.com/psirt/FG-IR-21-033

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.