Advisory Alert

Alert Number: AAA20220302 **Date:** March 2, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Fortinet	**Critical**	Multiple Vulnerabilities

Description

Affected Product	**Fortinet**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-22301, CVE-2022-22300, CVE-2021-36166, CVE-2021-32586, CVE-2022-22303, CVE-2020-15936, CVE-2021-36171, CVE-2021-44166, CVE-2021-43070, CVE-2021-43077, CVE-2021-43075)
Description	Fortinet has released Security Updates addressing multiple vulnerabilities that exists with Fortinet products. • CVE-2022-22301 - FortiAP-C - Command injection in CLI • CVE-2022-22300 - FortiAnalyzer, FortiManager - bypass of client-side password change policy enforcement • CVE-2021-36166 - FortiMail - Administrative authentication bypass • CVE-2021-32586 - FortiMail - Unsafe handling of CGI environment parameters in web server framework • CVE-2022-22303 - FortiManager - Password observed in cleartext in the config conflict file • CVE-2020-15936 - FortiOS - Bypassing FortiGate security profiles via SNI in Client Hello • CVE-2021-36171 - FortiPortal - Insecure password generation • CVE-2021-44166 - FortiToken Mobile (Android) - Deny request approved from External push notification • CVE-2021-43070 - FortiWLM - Path traversal vulnerability • CVE-2021-43077 - FortiWLM - SQL Injection in AP report handlers • CVE-2021-43075 - FortiWLM - command Injection in script handlers
Affected Products	FortiAP-C FortiAnalyzer FortiManager FortiMail Forti OS FortiPortal FortiToken Mobile (Android) FortiWLM
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-21-227 https://www.fortiguard.com/psirt/FG-IR-21-255 https://www.fortiguard.com/psirt/FG-IR-21-028 https://www.fortiguard.com/psirt/FG-IR-21-008 https://www.fortiguard.com/psirt/FG-IR-21-165 https://www.fortiguard.com/psirt/FG-IR-20-091 https://www.fortiguard.com/psirt/FG-IR-21-099 https://www.fortiguard.com/psirt/FG-IR-21-210 https://www.fortiguard.com/psirt/FG-IR-21-106 https://www.fortiguard.com/psirt/FG-IR-21-189 https://www.fortiguard.com/psirt/FG-IR-21-128

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.