Advisory Alert

Alert Number: AAA20220907 **Date:** September 7, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Fortinet	**High**, **Medium**	Multiple Vulnerabilities

Description

Affected Product	**Fortinet**	
Severity	**High**, **Medium**	
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-43076, CVE-2022-29058, CVE-2022-26114, CVE-2022-38377, CVE-2022-29053, CVE-2022-27491, CVE-2021-43080, CVE-2022-29061, CVE-2022-29062, CVE-2022-30298, CVE-2022-35847, CVE-2022-29059)	
Description	Fortigate has released security updates addressing multiple vulnerabilities that exists in their products including an improper privilege management, command injection, cross-site scripting, information leakage, improper verification, path traversal, privilege escalation, arbitrary code execute and SQL Injection. It is highly recommended by Fortigate to apply necessary security fixes at earliest to avoid issues.	
Affected Products	FortiADC version 6.2.1 and below. FortiADC version 6.1.5 and below. FortiADC version 6.0.4 and below. FortiADC version 5.4.5 and below. FortiADC version 5.3.7 and below. FortiAP-U version 5.4.0 through 5.4.6 FortiAP-U version 6.0.0 through 6.0.4 FortiAP-U version 6.2.0 through 6.2.3 FortiAP-W2 version 6.0.0 through 6.0.6 FortiAP-W2 version 6.2.0 through 6.2.6 FortiAP-W2 version 6.4.0 through 6.4.7 FortiAP-W2 version 7.0.0 through 7.0.3 FortiAP-W2 version 7.2.0 FortiAP-S version 6.0.0 through 6.0.6 FortiAP-S version 6.2.0 through 6.2.6 FortiAP-S version 6.4.0 through 6.4.7 FortiAP version 6.0.0 through 6.0.6 FortiAP version 6.4.3 through 6.4.7 FortiAP version 7.0.0 through 7.0.3 FortiAP version 7.2.0 FortiMail version 7.0.0 through 7.0.3 FortiMail version 6.4.0 through 6.4.7 FortiMail version 6.2.0 through 6.2.8	FortiMail version 6.0.0 through 6.0.12 FortiManager version 7.2.0 FortiManager version 7.0.0 through 7.0.3 FortiManager version 6.4.0 through 6.4.7 FortiManager version 6.2.0 through 6.2.9 FortiManager version 6.0.0 through 6.0.11 FortiAnalyzer version 7.2.0 FortiAnalyzer version 7.0.0 through 7.0.3 FortiAnalyzer version 6.4.0 through 6.4.8 FortiAnalyzer version 6.2.0 through 6.2.10 FortiAnalyzer version 6.0.0 through 6.0.12 FortiOS version 7.2.0 FortiOS version 6.4.0 through 6.4.8 FortiOS version 6.2.0 through 6.2.10 FortiOS version 6.0.0 through 6.0.14 FortiOS version 6.4.0 through 6.4.9 FortiOS version 7.0.0 through 7.0.5 FortiSOAR version 7.2.0 FortiSOAR version 6.4.1 through 6.4.4 FortiSOAR version 7.0.0 through 7.0.3 FortiSOAR version 6.4.0 through 6.4.4 FortiWeb version 6.2.3 through 6.2.7 FortiWeb version 6.3.0 through 6.3.18 FortiWeb version 6.4.0 through 6.4.2 FortiWeb version 7.0.0 through 7.0.1
Officially Acknowledged by the Vendor	Yes	
Patch/ Workaround Released	Yes	
Reference	https://www.fortiguard.com/psirt/FG-IR-21-215 https://www.fortiguard.com/psirt/FG-IR-21-163 https://www.fortiguard.com/psirt/FG-IR-21-045 https://www.fortiguard.com/psirt/FG-IR-20-143 https://www.fortiguard.com/psirt/FG-IR-22-158 https://www.fortiguard.com/psirt/FG-IR-22-073 https://www.fortiguard.com/psirt/FG-IR-21-222 https://www.fortiguard.com/psirt/FG-IR-22-156 https://www.fortiguard.com/psirt/FG-IR-22-154 https://www.fortiguard.com/psirt/FG-IR-22-152 https://www.fortiguard.com/psirt/FG-IR-22-306 https://www.fortiguard.com/psirt/FG-IR-22-140	

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.