Advisory Alert

Alert Number: AAA20210804 **Date:** August 4, 2021

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-2020-15939, CVE-2020-29011,CVE-2021-26098,CVE-2021-24010,CVE-2021-26096,CVE-2021-24014,CVE-2021-26097,CVE-2021-32602,CVE-2021-32596,CVE-2021-32594,CVE-2021-32590,CVE-2021-36168,CVE-2021-32588,CVE-2019-16151,CVE-2021-24018,CVE-2021-24006,CVE-2021-26104,CVE-2021-32597,CVE-2021-32603,CVE-2021-32587,CVE-2021-26097,CVE-2021-32598)
Description	Fortinet has released security updates addressing multiple vulnerabilities that exists in their products such as improper neutralization of CRLF sequences in HTTP headers, improper neutralization of special elements used in an OS Command, improper access control, server-side request forgery, multiple improper neutralization of input, multiple OS command injection, improper access control,buffer underwrite, authentication bypass, improper command execution as root, protection mechanism failure, multiple improper neutralization of special elements used in an SQL command, unrestricted file upload, use of one-way hash with a predictable salt, multiple instances of heap-based buffer overflow in the command shell, improper limitation of a pathname to a restricted directory and SQL Injection. Fortinet highly recommends to apply necessary security fixes to avoid issues.
Affected Products	FortiAnalyzer 6.4.x FortiAnalyzer version 6.4.5 and below. FortiAnalyzer versions 5.6.x, 6.2.x and 6.0.x also are impacted. FortiAnalyzer versions 6.2.7 and below. FortiAnalyzer versions 6.4.5 and below. FortiAnalyzer versions 7.0.0 FortiManager 6.4.x FortiManager version 6.4.5 and below. FortiManager versions 5.6.x, 6.2.x and 6.0.x are also impacted. FortiManager versions 6.2.7 and below. FortiManager versions 6.4.0 to 6.4.3. FortiManager versions 6.4.5 and below. FortiManager versions 7.0.0 FortiOS version 6.4.1 and below FortiOS version 6.4.6 and below. FortiOS version 7.0.0. FortiPortal 3.2.2 and below. FortiPortal 4.0.4 and below. FortiPortal 4.1.2 and below. FortiPortal 4.2.4 and below. FortiPortal 5.0.3 and below. FortiPortal 5.0.x FortiPortal 5.1.2 and below. FortiPortal 5.1.x FortiPortal versions 5.2.5 and below. FortiPortal versions 5.3.5 and below. FortiPortal versions 6.0.4 and below. FortiPortal versions 6.0.5 and below. FortiSandbox 3.0.6 and below. FortiSandbox version 3.1.4 and below. FortiSandbox version 3.2.1 and below. FortiSandbox version 3.2.2 and below. FortiSandbox version 3.2.2 and earlier.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-21-063 https://www.fortiguard.com/psirt/FG-IR-20-198 https://www.fortiguard.com/psirt/FG-IR-21-059 https://www.fortiguard.com/psirt/FG-IR-21-050 https://www.fortiguard.com/psirt/FG-IR-21-054 https://www.fortiguard.com/psirt/FG-IR-21-037 https://www.fortiguard.com/psirt/FG-IR-20-061 https://www.fortiguard.com/psirt/FG-IR-21-046 https://www.fortiguard.com/psirt/FG-IR-19-301 https://www.fortiguard.com/psirt/FG-IR-21-077 https://www.fortiguard.com/psirt/FG-IR-21-085 https://www.fortiguard.com/psirt/FG-IR-21-084 https://www.fortiguard.com/psirt/FG-IR-21-092 https://www.fortiguard.com/psirt/FG-IR-21-094 https://www.fortiguard.com/psirt/FG-IR-20-066 https://www.fortiguard.com/psirt/FG-IR-20-198 https://www.fortiguard.com/psirt/FG-IR-20-209 https://www.fortiguard.com/psirt/FG-IR-20-188 https://www.fortiguard.com/psirt/FG-IR-20-202 https://www.fortiguard.com/psirt/FG-IR-20-218 https://www.fortiguard.com/psirt/FG-IR-20-171 https://www.fortiguard.com/psirt/FG-IR-20-071

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.