Advisory Alert

Alert Number: AAA20220202 **Date:** February 2, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Fortigate	**High**	Multiple Vulnerabilities

Description

Affected Product	Fortigate	
Severity	**High**	
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-36177, CVE-2021-41016, CVE-2021-43062, CVE-2021-42753, CVE-2021-36193, CVE-2021-41018, CVE-2021-43073)	
Description	Fortigate has released security updates addressing multiple vulnerabilities that exists in their products including Improper access control , Arbitrary command execution, Cross site scripting , Path traversal, Stack-based buffer overflow and OS command injection. It is highly recommended by Fortigate to apply necessary security fixes at earliest to avoid issues.	
Affected Products	FortiAuthenticator 6.3.2 and below. FortiAuthenticator 6.2.x. FortiAuthenticator 6.1.x. FortiAuthenticator 6.0.x. FortiExtender version 7.0.1 and below. FortiExtender version 4.2.3 and below. FortiExtender version 4.1.7 and below. FortiMail version 7.0.1 and below FortiMail version 6.4.5 and below FortiMail version 6.2.7 and below FortiWeb 6.2.x, 6.1.x, 6.0.x, 5.9.x and 5.8.x.	FortiWeb 6.4.1 and earlier. FortiWeb 6.3.15 and earlier. FortiWeb 6.2.5 and earlier. FortiWeb 6.1.2 and earlier. FortiWeb 6.0.7 and earlier. All FortiWeb versions 5.x are also affected. FortiWeb version 6.3.15 and below FortiWeb version 6.4.1 and below FortiWeb version 6.3.16 and below FortiWeb version 6.2.6 and below
Officially Acknowledged by the Vendor	Yes	
Patch/ Workaround Released	Yes	
Reference	https://fortiguard.fortinet.com/psirt/FG-IR-20-217 https://fortiguard.fortinet.com/psirt/FG-IR-21-148 https://fortiguard.fortinet.com/psirt/FG-IR-21-185 https://fortiguard.fortinet.com/psirt/FG-IR-21-158 https://fortiguard.fortinet.com/psirt/FG-IR-21-132 https://fortiguard.fortinet.com/psirt/FG-IR-21-166 https://fortiguard.fortinet.com/psirt/FG-IR-21-180	

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.