Advisory Alert

Alert Number: AAA20221011 **Date:** October 11, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
FortiGuard	**Critical**	Multiple Vulnerabilities
VMware	**High**	Multiple Vulnerabilities
FortiGuard	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Intel	**High**, **Medium**	Multiple Vulnerabilities

Description

Affected Product	**FortiGuard**	
Severity	**Critical**	
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-40684, CVE-2022-33873)	
Description	FortiGuard has released Security Updates addressing multiple vulnerabilities that exist in their products. **CVE-2022-40684** – An authentication bypass using an alternate path or channel vulnerability that exists in FortiOS, FortiProxy and FortiSwitchManager. Using this vulnerability an unauthenticated attacker can perform operations on the administrative interface via specially crafted HTTP or HTTPS requests. **CVE-2022-33873** - Multiple improper neutralization of special elements used in an OS Command ('OS Command Injection') vulnerabilities that exist in Console, Telnet, and SSH login components of FortiTester. Using this vulnerability an unauthenticated remote attacker can execute arbitrary command in the underlying shell. FortiGuard highly recommends to apply the necessary patch updates at your earliest to avoid issues.	
Affected Products	FortiOS version 7.2.0 through 7.2.1 FortiOS version 7.0.0 through 7.0.6 FortiProxy version 7.2.0 FortiProxy version 7.0.0 through 7.0.6 FortiSwitchManager version 7.2.0 FortiSwitchManager version 7.0.0 FortiTester version 7.1.0 FortiTester version 7.0.0 FortiTester version 4.2.0 FortiTester version 4.1.0 through 4.1.1 FortiTester version 4.0.0 FortiTester version 3.9.0 through 3.9.1 FortiTester version 3.8.0 FortiTester version 3.7.0 through 3.7.1	FortiTester version 3.6.0 FortiTester version 3.5.0 through 3.5.1 FortiTester version 3.4.0 FortiTester version 3.3.0 through 3.3.1 FortiTester version 3.2.0 FortiTester version 3.1.0 FortiTester version 3.0.0 FortiTester version 2.9.0 FortiTester version 2.8.0 FortiTester version 2.7.0 FortiTester version 2.6.0 FortiTester version 2.5.0 FortiTester version 2.4.0 through 2.4.1 FortiTester version 2.3.0
Officially Acknowledged by the Vendor	Yes	
Patch/ Workaround Released	Yes	
Reference	https://www.fortiguard.com/psirt/FG-IR-22-377 https://www.fortiguard.com/psirt/FG-IR-22-237	

Affected Product	**VMware**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-31680, CVE-2022-31681)
Description	VMware has released a security update addressing multiple vulnerabilities that exists in their VMware ESXi, vCenter Server and VMware Cloud Foundation **CVE-2022-31680** - Unsafe deserialisation vulnerability that exists in the PSC (Platform services controller). Using this vulnerability an attacker with admin privileges can execute arbitrary code on the underlying operating system that hosts the vCenter Server. **CVE-2022-31681 -** A null-pointer dereference vulnerability that exist in the VMware ESXi. Using this vulnerability a malicious actor with privileges within the VMX process only, may create a denial of service condition on the host. VMware highly recommends to apply the necessary patch updates at your earliest to avoid issues
Affected Products	VMware vCenter Server version 6.5 with an external PSC VMware ESXi version 7.0, 6.7 and 6.5 VMware Cloud Foundation (ESXi) version 4.x and 3.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.vmware.com/security/advisories/VMSA-2022-0025.html

Affected Product	**FortiGuard**	
Severity	**High**, **Medium**, **Low**	
Affected Vulnerability	Multiple Vulnerabilities(CVE-2022-26121, CVE-2021-44171, CVE-2022-29055, CVE-2022-35844, CVE-2022-35846)	
Description	FortiGuard has released security updates addressing multiple vulnerabilities that exists in their products. Successful exploitation of these vulnerabilities could cause accessing report template images and guessing credentials of the admin users via brute force attacks because of the improper access control, Execution of unauthorized code or commands and Denial of service. FortiGuard highly recommends to apply the necessary patch updates at your earliest to avoid issues	
Affected Products	FortiManager version 7.0.0 through 7.0.3 FortiManager version 6.4.0 through 6.4.8 FortiManager version 6.2.0 through 6.2.9 FortiManager version 6.0.0 through 6.0.11 FortiManager version 5.6.0 through 5.6.11 FortiAnalyzer version 7.0.0 through 7.0.3 FortiAnalyzer version 6.4.0 through 6.4.8 FortiAnalyzer version 6.2.0 through 6.2.9 FortiAnalyzer version 6.0.0 through 6.0.11 FortiAnalyzer version 5.6.0 through 5.6.11 FortiOS version 6.0.0 through 6.0.14 FortiOS version 6.2.0 through 6.2.10 FortiOS version 6.4.0 through 6.4.8 FortiOS version 7.0.0 through 7.0.3 No need to be authenticated to provoke a crash: FortiOS version 6.4.4 through 6.4.9 FortiOS version 7.0.0 through 7.0.5 FortiOS version 7.2.0 FortiProxy version 7.0.0 through 7.0.4 Need to be authenticated to provoke a crash: FortiOS version 6.4.0 through 6.4.3 FortiProxy version 1.2.6 through 1.2.13 FortiProxy version 2.0.0 through 2.0.9 FortiTester version 7.1.0	FortiTester version 7.0.0 FortiTester version 4.2.0 FortiTester version 4.1.0 through 4.1.1 FortiTester version 4.0.0 FortiTester version 3.9.0 through 3.9.1 FortiTester version 3.8.0 FortiTester version 3.7.0 through 3.7.1 FortiTester version 3.6.0 FortiTester version 3.5.0 through 3.5.1 FortiTester version 3.4.0 FortiTester version 3.3.0 through 3.3.1 FortiTester version 3.2.0 FortiTester version 3.1.0 FortiTester version 3.0.0 FortiTester version 2.9.0 FortiTester version 2.8.0 FortiTester version 2.7.0 FortiTester version 2.6.0 FortiTester version 2.5.0 FortiTester version 2.4.0 through 2.4.1 FortiTester version 2.3.0 FortiTester version 7.1.0 through 7.1.1 FortiTester version 4.2.0 through 4.2.1 FortiTester version 3.9.0 through 3.9.2
Officially Acknowledged by the Vendor	Yes	
Patch/ Workaround Released	Yes	
Reference	https://www.fortiguard.com/psirt/FG-IR-22-026 https://www.fortiguard.com/psirt/FG-IR-21-242 https://www.fortiguard.com/psirt/FG-IR-22-086 https://www.fortiguard.com/psirt/FG-IR-22-247 https://www.fortiguard.com/psirt/FG-IR-22-244	

Affected Product	**Intel**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities(CVE-2021-33060, CVE-2022-26074)
Description	Intel has released a firmware updates to address multiple vulnerabilities that can affect the Intel processors. **CVE-2021-33060** – A vulnerability that exist in the BIOS firmware for some Intel Processors because of an Out-of-bounds write in the BIOS firmware. Using this vulnerability an unauthenticated attacker can execute privilege escalation via local access. **CVE-2022-26074** – A vulnerability that exists because of an Incomplete cleanup flaw in a firmware subsystem for Intel SPS before versions SPS_E3_04.08.04.330.0 and SPS_E3_04.01.04.530.0. Using this vulnerability a privileged user can enable denial of service via local access. Intel highly recommends to apply the necessary firmware updates at your earliest to avoid issues
Affected Products	3rd Generation Intel Xeon Scalable Processor Family Intel SPS before version SPS_E3_04.08.04.330.0 and SPS_E3_04.01.04.530.0.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00669.html https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00686.html

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.