Advisory Alert

Alert Number: AAA20230217 **Date:** February 17, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Fortiguard	**Critical**	Multiple Vulnerabilities
Joomla	**High**	Incorrect Access Control Vulnerability
Fortiguard	**High , Medium**	Multiple Vulnerabilities
Dell	**High , Medium**	Multiple Vulnerabilities
IBM	**Medium , Low**	Multiple Vulnerabilities

Description

Affected Product	**Fortiguard**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-42756, CVE-2022-39952)
Description	Fortiguard has released security updates addressing multiple vulnerabilities that exist in their products. Attackers can exploit these vulnerabilities to cause arbitrary code execution and arbitrary write. **CVE-2021-42756-** A vulnerability in FortiWeb's proxy daemon may allow an unauthenticated remote attacker to achieve arbitrary code execution via specifically crafted HTTP requests. **CVE-2021-42756-** A vulnerability in FortiNAC webserver may allow an unauthenticated attacker to perform arbitrary write on the system. Fortiguard highly recommends to apply necessary fixes to avoid issues.
Affected Products	FortiNAC version 9.4.0 FortiNAC version 9.2.0 through 9.2.5 FortiNAC version 9.1.0 through 9.1.7 FortiNAC 8.8 all versions FortiNAC 8.7 all versions FortiNAC 8.6 all versions FortiNAC 8.5 all versions FortiNAC 8.3 all versions FortiWeb versions 5.x all versions, FortiWeb versions 6.0.7 and below, FortiWeb versions 6.1.2 and below, FortiWeb versions 6.2.6 and below, FortiWeb versions 6.3.16 and below, FortiWeb versions 6.4 all versions.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-22-300 https://www.fortiguard.com/psirt/FG-IR-21-186

Affected Product	**Joomla**
Severity	**High**
Affected Vulnerability	Incorrect Access Control Vulnerability (CVE-2023-23752)
Description	Joomla has released a security update addressing Incorrect Access Control Vulnerability exists due to improper access restrictions to Web Service endpoints. A remote attacker can bypass implemented security restrictions and compromise the web application. Joomla recommends to apply necessary fixes to avoid issues.
Affected Products	Joomla CMS versions 4.0.0-4.2.7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://developer.joomla.org/security-centre/894-20230201-core-improper-access-check-in-webservice-endpoints.html

Affected Product	**Fortiguard**	
Severity	**High**, **Medium**	
Affected Vulnerability	Multiple vulnerabilities (CVE-2021-43074, CVE-2022-22302, CVE-2022-26115, CVE-2022-27482, CVE-2022-27489, CVE-2022-29054, CVE-2022-30299, CVE-2022-30300, CVE-2022-30303, CVE-2022-30304, CVE-2022-30306, CVE-2022-33869, CVE-2022-33871, CVE-2022-38375, CVE-2022-38376, CVE-2022-38378, CVE-2022-39948, CVE-2022-39954, CVE-2022-40675, CVE-2022-40677, CVE-2022-40678, CVE-2022-40683, CVE-2022-41334, CVE-2022-41335, CVE-2022-42472, CVE-2022-43954, CVE-2023-22638, CVE-2023-23777, CVE-2023-23778, CVE-2023-23779, CVE-2023-23780, CVE-2023-23781, CVE-2023-23782, CVE-2023-23784, CVE-2023-25602)	
Description	Fortiguard has released security updates addressing multiple vulnerabilities that exist in their products. If exploited these vulnerabilities could lead to cross-site scripting vulnerabilities, XML external entity injection, Privilege escalation. Fortiguard recommends to apply necessary fixes to avoid issues.	
Affected Products	FortiADC 5.0 -5.4 all versions FortiADC 6.0 all versions FortiADC 6.1 all versions FortiADC version 6.2.0 through 6.2.2 FortiADC version 7.0.0 through 7.0.2 FortiAnalyzer version 6.0.0 through 6.0.11 FortiAnalyzer version 6.2.0 through 6.2.9 FortiAnalyzer version 6.4.0 through 6.4.8 FortiAnalyzer version 7.0.0 through 7.0.4 FortiAnalyzer version 7.2.0 through 7.2.1. FortiAuthenticator 5.5 all versions FortiAuthenticator version 6.0.0 through 6.0.4 FortiAuthenticator version 6.1.0 FortiExtender 3.0 all versions FortiExtender 3.1 all versions FortiExtender 5.3 all versions FortiExtender version 3.2.1 through 3.2.3 FortiExtender version 3.3.0 through 3.3.2 FortiExtender version 4.0.0 through 4.0.2 FortiExtender version 4.1.1 through 4.1.8 FortiExtender version 4.2.0 through 4.2.4 FortiExtender version 7.0.0 through 7.0.3 FortiNAC 8.8, 8.7, 8.6, 8.5, 8.3 all versions FortiNAC all versions 9.2, 9.1, 8.8, 8.7, 8.6, 8.5, 8.3 FortiNAC version 9.1.0 through 9.1.7 FortiNAC version 9.2.0 through 9.2.6 FortiNAC version 9.4.0 through 9.4.1 FortiOS 6.0 all versions FortiOS 6.2 all versions FortiOS 6.4 all versions	FortiOS version 7.0.0 through 7.0.8 FortiOS version 7.2.0 through 7.2.3 FortiOS versions 6.4.8 and below, FortiOS versions 7.0.3 and below. FortiPortal version 7.0.0 through 7.0.2 FortiProxy 1.0 all versions FortiProxy 2.0 all versions FortiProxy version 7.0.0 through 7.0.6 FortiProxy version 7.0.0 through 7.0.7 FortiProxy version 7.2.0 through 7.2.1 FortiProxy versions 2.0.7 and below, FortiProxy versions 7.0.1 and below, FortiSandbox version 3.2.0 through 3.2.3 FortiSandbox version 4.0.0 through 4.0.2 FortiSwitch 6.0 all versions FortiSwitch 6.2 all versions FortiSwitch versions 6.4.10 and below, FortiSwitch versions 7.0.3 and below, FortiSwitchManager version 7.0.0 FortiSwitchManager version 7.2.0 FortiWAN version 4.0.0 through 4.0.6 FortiWAN version 4.1.1 through 4.1.3 FortiWAN version 4.2.1 through 4.2.2 FortiWAN version 4.2.5 through 4.2.7 FortiWAN version 4.3.0 through 4.3.1 FortiWAN version 4.4.0 through 4.4.1 FortiWAN version 4.5.0 through 4.5.9 FortiWeb 5.6 - 6.4 all versions FortiWeb version 7.0.0 through 7.0.3 FortiWeb versions 6.3.20 and earlier.
Officially Acknowledged by the Vendor	Yes	
Patch/ Workaround Released	Yes	
Reference	https://www.fortiguard.com/psirt?page=1 https://www.fortiguard.com/psirt?page=2 https://www.fortiguard.com/psirt?page=3	

Affected Product	**Dell**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple vulnerabilities (CVE-2022-40262 , CVE-2019-14553, CVE-2021-0200)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in their products. If exploited these vulnerabilities could lead to Privilege escalation, arbitrary code execution, and information disclosure. **CVE-2021-40262 -** An attacker can execute an arbitrary code at the time of the PEI phase and influence the subsequent boot stages which can lead to mitigations bypassing, physical memory contents disclosure and build a payload which can be injected into the SMRAM memory. **CVE-2019-14553-** Improper authentication in EDK II may allow a privileged user to potentially enable information disclosure via network access. **CVE-2021-0200-** Arbitrary code execution vulnerability in Intel Ethernet controllers caused by an out-of-bounds write flaw in the firmware. An authenticated attacker could exploit this vulnerability by sending a specially-crafted request. Dell recommends to apply the necessary security updates at earliest to avoid issues.
Affected Products	Dell Networking VEP4600 4-Core Dell Networking VEP4600 8-Core Alienware Area 51m R1,Aurora R10,Aurora R8,Aurora R9,m15 R1,m15 R2,m17 R1,m17 R2 ChengMing 3980 TOWER ChengMing 3988 Dell G3 3579 Dell G3 3779 Dell G5 5090 Dell Networking VEP4600 16-Core Dell 3430 Tower Dell 3431 Tower Dell 3630 Tower Dell 3930 Rack Dell 7820 Tower Dell 7920 Tower Edge Gateway 3000 series Edge Gateway 5000 (Commercial) Embedded Box PC 3000 Embedded Box PC 5000 Inspiron 3280, 3470, 3471, 3480, 3481, 3482, 3502, 3580, 3581, 3582, 3670, 3671, 3780, 3781, 3782, 5570, 5770 Latitude 12 Rugged Extreme 7214, 12 Rugged Tablet 7212, 14 Rugged 5414, 3180, 3189, 3190, 3190 2-in-1, 3380, 3390, 3480, 3490, 3580, 3590, 5280, 5288, 5289, 5290, 5480, 5488, 5490, 5491, 5580, 5590, 5591, 7280, 7290, 7370, 7380, 7389, 7390, 7414 Rugged Extreme, 7480, 7490, Rugged 5420, Rugged 5424, Rugged 7424 OptiPlex 3050 AIO19.5 Display, 3050MT/SFF/Micro, 3060, 3070, 5050MT/SFF/Micro, 5060, 5070, 5250, 5260 All-in-One, 5270 All-in-One, 7050MT/SFF/Micro, 7060, 7070, 7070 UFF, 7071, 7450 AIO23.8 Display, 7460 All-In-One, 7470 All-in-One, 7760 AIO, 7770 All-in-One, XE3 Precision 3420 Tower, 3520, 3530, 3620 Tower, 5520, 5530 2-in-1, 5720 AIO, 7510, 7520, 7530, 7540, 7710, 7720, 7730, 7740 Vostro 3070, 3267, 3268, 3470, 3471, 3480, 3481, 3582, 3583 (1SP) / 3580 (2SP), 3584 (1SP) / 3581 (2SP), 3667, 3668, 3669, 3670, 3671, 5090 Wyse 5070 Wyse 5470 Wyse 5470 All-In-One Wyse 7040 Thin Client XPS 15 9575 2-in-1 XPS 8930
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000208382/dsa-2023-050 https://www.dell.com/support/kbdoc/en-us/000209538/dsa-2023-079-dell-security-update-for-a-networking-bios-vulnerability https://www.dell.com/support/kbdoc/en-us/000209536/dsa-2023-078-dell-emc-networking-bios-security-update-for-multiple-vulnerabilities

Affected Product	**IBM**
Severity	**Medium**, **Low**
Affected Vulnerability	Multiple vulnerabilities (CVE-2021-0197, CVE-2021-0198, CVE-2021-0199, CVE-2021-0200)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in third party tools in their products. Attackers can exploit these vulnerabilities to cause denial of service and privilege escalation. **CVE-2021-0197-** Denial of service vulnerability in Intel Ethernet controllers caused by an improper access control in the firmware. A local authenticated attacker could exploit this vulnerability by sending a specially-crafted request. **CVE-2021-0198-** Denial of service vulnerability in Intel Ethernet controllers caused by a protection mechanism failure in the firmware. A local authenticated attacker could exploit this vulnerability by sending a specially-crafted request. **CVE-2021-0199-** Denial of service vulnerability in Intel Ethernet controllers caused by an improper input validation in the firmware. A local authenticated attacker could exploit this vulnerability by sending a specially-crafted request. **CVE-2021-0200-** Privilege escalation vulnerability in Intel Ethernet controllers caused by an out-of-bounds write flaw in the firmware. An authenticated attacker could exploit this vulnerability by sending a specially-crafted request. IBM recommends to apply necessary fixes to avoid issues
Affected Products	IBM QRadar SIEM 7.4.0 - 7.4.3 Fix Pack 6 IBM QRadar SIEM 7.5.0 - 7.5.0 Update Pack 2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6956287

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.