Advisory Alert

Alert Number: AAA20230104 **Date:** January 4, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

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

Description

Affected Product	**Fortinet**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple vulnerabilities (CVE-2022-39947, CVE-2022-45857, CVE-2022-41336, CVE-2022-35845)
Description	Fortinet has released security updates addressing multiple vulnerabilities that exist in their products. If exploited, these vulnerabilities can lead to unauthorized code or command execution, FortiGate access without password, cross site scripting (XSS) and injection of arbitrary headers. Fortinet highly recommends to apply necessary fixes to avoid issues.
Affected Products	FortiADC version 7.0.0 through 7.0.2 FortiADC version 6.2.0 through 6.2.3 FortiADC version 6.1.0 through 6.1.6 FortiADC version 6.0.0 through 6.0.4 FortiADC version 5.4.0 through 5.4.5 FortiManager version 7.0.0 through 7.0.1 FortiManager version 6.4.0 through 6.4.7 FortiManager version 6.2.0 through 6.2.9 FortiPortal version 6.0.0 through 6.0.11 FortiPortal 5.3 all versions FortiPortal 5.2 all versions FortiPortal 5.1 all versions FortiPortal 5.0 all versions FortiTester version 7.1.0 FortiTester version 7.0 all versions FortiTester version 4.0.0 through 4.2.0 FortiTester version 2.3.0 through 3.9.1 FortiWeb version 7.0.0 through 7.0.2 FortiWeb version 6.4.0 through 6.4.2 FortiWeb version 6.3.6 through 6.3.20
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-22-061 https://www.fortiguard.com/psirt/FG-IR-22-371 https://www.fortiguard.com/psirt/FG-IR-22-313 https://www.fortiguard.com/psirt/FG-IR-22-274 https://www.fortiguard.com/psirt/FG-IR-22-250

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple vulnerabilities (CVE-2014-3566, CVE-2014-3568, CVE-2016-0705, CVE-2017-3732, CVE-2017-3736, CVE-2018-1428, CVE-2018-1427, CVE-2018-1426, CVE-2018-1447)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. If exploited, these vulnerabilities can lead to denial of service, security restriction bypass, sensitive information disclosure, duplicate Session IDs and key materials. IBM highly recommends to apply necessary fixes to avoid issues.
Affected Products	IBM Websphere Message Broker V7.0 and V8.0 IBM Integration Bus V9.0 IBM WebSphere Message Broker Hypervisor Edition V8.0 IBM Integration Bus Hypervisor Edition V9.0 IBM SOA Policy pattern for Red Hat Enterprise Linux Server WebSphere MQ v7.0.1 WebSphere MQ v7.1 WebSphere MQ v7.5 IBM MQ v8.0 and IBM MQ Appliance v8.0 IBM MQ v9.0 LTS IBM MQ v9.0.x CD and IBM MQ Appliance v9.0.x CD
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/254373 https://www.ibm.com/support/pages/node/711755

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.