Advisory Alert

Alert Number: AAA20210428 **Date:** April 28, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Fortigate	Critical	Path traversal vulnerability
IBM	High	Multiple vulnerabilities

Description

Affected Product	Fortigate
Severity	**Critical**
Affected Vulnerability	Path traversal vulnerability (CVE-2021-26102)
Description	A relative Path traversal vulnerability in FortiWAN may allow a remote non-authenticated attacker to delete arbitrary files on the system using directory traversal sequences on the system by sending a crafted POST request. In particular, deleting specific configuration files will reset the Admin password to its default value.
Affected Products	FortiWAN versions 4.5.7 and below.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-21-048

Affected Product	IBM
Severity	**High**
Affected Vulnerability	Multiple vulnerabilities (CVE-2021-20353, CVE-2021-20354, CVE-2020-5016, CVE-2020-4949)
Description	IBM has released security patch update addressing vulnerabilities that exist in WebSphere Application Server product such as **CVE-2021-20353,CVE-2020-4949** - IBM WebSphere Application Server is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker can exploit this vulnerability to expose sensitive information or consume memory resources **CVE-2021-20354 -** IBM WebSphere Application Server could allow a remote attacker to traverse directories. An attacker could send a specially created URL base request including dot sequences to view arbitrary files on the system **CVE-2020-5016 -** IBM WebSphere Application Server could allow a remote attacker to traverse directories on the system. When application security is disabled and JAX-RPC applications are included, an attacker could send a specially created URL base request containing dot sequences to view arbitrary XML files on the system.
Affected Products	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6446231

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.