Advisory Alert

Alert Number: AAA20221213 **Date:** December 13, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Fortinet	**Critical**	Heap-based buffer overflow Vulnerability
IBM	**Critical**	Arbitrary Code Execution Vulnerability
IBM	**High**	Denial Of Service Vulnerability
Ubuntu	**High**, **Medium**, **Low**	Multiple Vulnerabilities

Description

Affected Product	**Fortinet**
Severity	**Critical**
Affected Vulnerability	Heap-based buffer overflow Vulnerability (CVE-2022-42475)
Description	Fortinet has released a Security Update addressing a heap-based buffer overflow Vulnerability that exist in the FortiOS **CVE-2022-42475** - A remote unauthenticated attacker could execute arbitrary code or commands via specifically crafted requests. Fortinet highly recommends to apply necessary security updates at earliest to avoid issues.
Affected Products	FortiOS version 7.2.0 through 7.2.2 FortiOS version 7.0.0 through 7.0.8 FortiOS version 6.4.0 through 6.4.10 FortiOS version 6.2.0 through 6.2.11 FortiOS-6K7K version 7.0.0 through 7.0.7 FortiOS-6K7K version 6.4.0 through 6.4.9 FortiOS-6K7K version 6.2.0 through 6.2.11 FortiOS-6K7K version 6.0.0 through 6.0.14
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-22-398

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Arbitrary code execution Vulnerability (CVE-2022-40674)
Description	IBM has released a Security Update addressing an arbitrary code execution Vulnerability that exist in the Expat library for IBM Db2 Net Search Extender. **CVE-2022-40674** – An arbitrary code execution Vulnerability exist in the Expat library, caused by a use-after-free in the doContent function in xmlparse.c. A remote attacker could exploit this vulnerability to execute arbitrary code on the system. IBM highly recommends to apply necessary security updates at earliest to avoid issues.
Affected Products	All fix pack levels of IBM Db2 V9.7, V10.1, V10.5, and V11.1 server editions on all platforms are affected.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6847293

Affected Product	**IBM**
Severity	**High**
Affected Vulnerability	Denial Of Service Vulnerability (CVE-2022-43680)
Description	IBM has released a Security Update addressing a denial of service Vulnerability that exist in the Expat library for IBM Db2 Net Search Extender. **CVE-2022-43680 -** A denial of service vulnerability exist in the Expat library, caused by a use-after free created by overeager destruction of a shared DTD in XML_ExternalEntityParserCreate in out-of-memory situations. A remote attacker could exploit this vulnerability to cause a denial of service. IBM highly recommends to apply necessary security updates at earliest to avoid issues.
Affected Products	All fix pack levels of IBM Db2 V9.7, V10.1, V10.5, and V11.1 server editions on all platforms are affected.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6847293

Affected Product	**Ubuntu**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-3621, CVE-2022-42703, CVE-2022-2978, CVE-2022-20422, CVE-2022-3239, CVE-2022-36879, CVE-2022-3566, CVE-2022-3564, CVE-2022-40768, CVE-2022-3594, CVE-2022-3635, CVE-2022-2153,CVE-2022-3567, CVE-2022-3028, CVE-2022-3565, CVE-2022-3524, CVE-2022-43945, CVE-2022-33743, CVE-2022-26365)
Description	Ubuntu has released Security Updates addressing multiple vulnerabilities that affect Linux Kernel packages. If exploited these vulnerabilities could lead to denial of service or arbitrary code execution, sensitive information disclosure and undesired behaviors Ubuntu recommends to apply necessary security fixes at earliest to avoid issues
Affected Products	Ubuntu 22.10 Ubuntu 22.04 Ubuntu 18.04 Ubuntu 14.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-5754-2 https://ubuntu.com/security/notices/USN-5773-1 https://ubuntu.com/security/notices/USN-5756-3 https://ubuntu.com/security/notices/USN-5774-1

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.