Advisory Alert

Alert Number: AAA20240326 **Date:** March 26, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

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

Description

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-44487,CVE-2023-47746,CVE-2015-8391,CVE-2023-47145,CVE-2023-27859,CVE-2002-0059,CVE-2023-50308,CVE-2020-14155,CVE-2023-47158,CVE-2023-47701,CVE-2015-8388,CVE-2023-29258,CVE-2023-47747,CVE-2023-47152,CVE-2022-3510,CVE-2023-38727,CVE-2015-8387,CVE-2022-37434,CVE-2015-8381,CVE-2023-32731,CVE-2023-46167,CVE-2023-47141,CVE-2015-8392,CVE-2022-3171,CVE-2023-44483,CVE-2018-25032,CVE-2022-3509,CVE-2015-8385,CVE-2015-2327,CVE-2023-43020,CVE-2023-1370,CVE-2015-8390,CVE-2023-40687,CVE-2023-45193,CVE-2015-8393,CVE-2023-43642,CVE-2023-38003,CVE-2015-8394,CVE-2023-45178,CVE-2023-34462,CVE-2015-2328,CVE-2023-40692,CVE-2015-8395,CVE-2015-8383,CVE-2015-8386)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in IBM Db2 and IBM WebSphere products that in turn affect IBM Storage Protect Operations Center and Storage Protect Server. An attacker may exploit these vulnerabilities which could lead to Denial of service, Information disclosure, Execute arbitrary code. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Storage Protect Server - Version 8.1.0.000 - 8.1.21.XXX IBM Storage Protect Operations Center - Version 8.1.0.000 - 8.1.21.XXX
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7144914 https://www.ibm.com/support/pages/node/7144912 https://www.ibm.com/support/pages/node/7144858 https://www.ibm.com/support/pages/node/7144910

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.