Advisory Alert

Alert Number: AAA20230331 **Date:** March 31, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
IBM	**Critical**	Multiple Vulnerabilities
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-25941, CVE-2023-25940, CVE-2023-25942, CVE-2019-15876,CVE-2022-26377, CVE-2022-28330, CVE-2022-28614, CVE-2022-28615, CVE-2022-29404, CVE-2022-30522, CVE-2022-30556, CVE-2022-31813)
Description	Dell has released a security update addressing multiple vulnerabilities that exists in Dell EMC PowerScale OneFS and some third party components that used by the product. Exploitation of the most severe vulnerabilities could cause privilege escalation, denial of service, and request smuggling. Dell highly recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	PowerScale OneFS version 9.1.0.0 to 9.5.0.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000211539/dell-emc-powerscale-onefs-security

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-37601, CVE-2022-37598, CVE-2021-42581, CVE-2021-39227, CVE-2020-15366, CVE-2021-3918, CVE-2021-42740, CVE-2021-23450, CVE-2022-36364, CVE-2020-13936, CVE-2022-4883)
Description	IBM has released a security update addressing multiple critical vulnerabilities that exist in the components that used by the IBM Qradar User Behavior Analytics and Qradar SIEM. If exploited these vulnerabilities could cause arbitrary code execution, and Denial of service. IBM highly recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	IBM QRadar SIEM Versions - 7.5.0 to 7.5.0 UP4 IBM QRadar SIEM Versions - 7.4.3 GA - 7.4.3 FP8 IBM QRadar User Behavior Analytics Versions 1.0.0 - 4.1.10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6967283 https://www.ibm.com/support/pages/node/6967333

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2019-6283, CVE-2018-20821, CVE-2020-24025, CVE-2018-19838, CVE-2018-11694, CVE-2018-19827, CVE-2018-20190, CVE-2019-6286, CVE-2019-6284, CVE-2018-19839, CVE-2018-19797, CVE-2022-37603, CVE-2021-3765, CVE-2022-31129, CVE-2022-24785, CVE-2021-23343, CVE-2021-23382, CVE-2022-25927, CVE-2022-37599, CVE-2022-24999, CVE-2021-32803, CVE-2021-37712, CVE-2021-37701, CVE-2021-37713, CVE-2021-32804, CVE-2020-7764, CVE-2021-23364, CVE-2022-25758, CVE-2021-23362, CVE-2021-23368, CVE-2021-29060, CVE-2022-25901, CVE-2021-3807, CVE-2021-25220, CVE-2022-2795, CVE-2022-42252, CVE-2022-40149, CVE-2022-40150, CVE-2022-21628, CVE-2022-21626, CVE-2022-21624, CVE-2022-21619, CVE-2022-45143, CVE-2022-24839, CVE-2022-46363, CVE-2018-8036, CVE-2022-41946, CVE-2022-41704, CVE-2022-23437, CVE-2022-25647, CVE-2022-22971, CVE-2022-22970, CVE-2019-10785, CVE-2020-5259, CVE-2018-15494, CVE-2022-21724, CVE-2022-31197, CVE-2022-41966, CVE-2022-42890, CVE-2022-28733, CVE-2023-22809, CVE-2022-46364, CVE-2021-26401, CVE-2022-2964, CVE-2022-4254, CVE-2022-40152, CVE-2022-40153, CVE-2022-40154, CVE-2022-40155, CVE-2022-40156, CVE-2022-34917, CVE-2022-3676, CVE-2022-36033, CVE-2021-37136, CVE-2021-37137, CVE-2021-43797, CVE-2021-21295, CVE-2021-21409, CVE-2021-21290, CVE-2022-24823, CVE-2022-41715, CVE-2022-30580, CVE-2022-1962, CVE-2022-30629, CVE-2022-2879, CVE-2022-30630, CVE-2022-32148, CVE-2022-30635, CVE-2022-30633, CVE-2022-27664, CVE-2022-1705, CVE-2022-2880, CVE-2022-28131, CVE-2022-30631, CVE-2022-32189, CVE-2022-30632,
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. If exploited most severe vulnerabilities of these vulnerabilities could cause application crash, Security Restriction bypass, denial of service, arbitrary moment switch, arbitrary code execution, arbitrary file write, security restriction bypass, sensitive information disclosure, and cookie based authentication information, backend information manipulation. IBM recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	IBM QRadar SIEM Versions - 7.5.0 to 7.5.0 UP4 IBM QRadar SIEM Versions - 7.4.3 GA - 7.4.3 FP8 IBM QRadar User Behavior Analytics Versions 1.0.0 - 4.1.10 IBM WebSphere Automation up to and including version 1.5.1.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6967283 https://www.ibm.com/support/pages/node/6967333 https://www.ibm.com/support/pages/node/6966998

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.