Advisory Alert

Alert Number: AAA20210312 **Date:** March 12, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	High	Multiple Vulnerabilities
Redhat	High	Code execution vulnerability
PaloAlto	Medium	Information Disclosure

Description

Affected Product	IBM
Severity	High
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-5024, CVE-2020-4976)
Description	IBM has released security updates addressing multiple vulnerabilities that exists in IBM DB2 products. CVE-2020-5024: An unauthenticated attacker could cause denial of service using a flaw that occurs due to hang in the SSL handshake response. CVE-2020-4976: A local user could read and write specific files due to weak file permission flaw that exists in IBM DB2.
Affected Products	IBM Db2 V9.7, V10.1, V10.5, V11.1, and V11.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6427861 https://www.ibm.com/support/pages/node/6427859

Affected Product	Redhat
Severity	High
Affected Vulnerability	Code execution vulnerability (CVE-2021-27803)
Description	Redhat has released security updates addressing a vulnerability that exits in wpa_supplicant. Using this flaw an attacker who is within the radio range of device running P2P discovery could cause code execution or terminate the wpa-supplicant process.
Affected Products	Red Hat Enterprise Linux 7 Red Hat Enterprise Linux 8
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/security/cve/CVE-2021-27803

Affected Product	PaloAlto
Severity	Medium
Affected Vulnerability	Information Disclosure (CVE-2021-3034)
Description	PaloAlto has released security updates addressing vulnerability that exists in their products. The flaw exists due to software stores secrets configured for the SAML single sign-on (SSO) integration into the '/var/log/demisto/' server log files, when testing the integration during setup. A local user can read the log files and gain access to sensitive data.
Affected Products	Cortex XSOAR 5.5.0 builds earlier than 98622 Cortex XSOAR 6.0.1 builds earlier than 830029 Cortex XSOAR 6.0.2 builds earlier than 98623 Cortex XSOAR 6.1.0 builds earlier than 848144
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.paloaltonetworks.com/CVE-2021-3034

Financial Sector Computer Security Incident Response Team (FinCSIRT)
LankaClear Pvt Ltd, Level 18, Bank of Ceylon Head Office, BOC Square, 01 Bank of Ceylon Mawatha, Colombo 00100, Sri Lanka
Hotline: + 94 112039777