Advisory Alert

Alert Number : AAA20210420 **Date :** April 20, 2021

Document Classification Level : Public Circulation Permitted

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
VMware	High	Privilege Escalation Vulnerability
IBM	High	Multiple Vulnerabilities
		XML External Entity (XXE) Injection vulnerability
Red Hat	High	Nettle signature verification functionality failure
Hewlett Packard	High	Multiple Vulnerabilities
WordPress	High	Multiple Vulnerabilities

Description

Affected Product	VMware
Severity	High
Affected Vulnerability	privilege escalation vulnerability(CVE-2021-21981)
Description	A privilege escalation vulnerability is discovered in VMware NSX-T as a result of an issue with RBAC (Role based access control) role assignment. Attackers with local guest user account will be able to gain higher privileges than their own permission level upon a successful exploitation of this issue.
Affected Products	VMware NSX-T
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.vmware.com/security/advisories/VMSA-2021-0006.html

Affected Product	IBM
Severity	High
Affected Vulnerabilities	Multiple Vulnerabilities(CVE-2020-4230, CVE-2020-4135, CVE-2020-4204, CVE-2020-4200, CVE-2020-4161, CVE-2017-12973, CVE-2017-12972, CVE-2018-8012, CVE-2017-5637, CVE-2018-11771, CVE-2018-10237, CVE-2018-8009, CVE-2016-2402, CVE-2009-0001, CVE-2019-9512, CVE-2019-9514, CVE-2019-9515, CVE-2019-9518, CVE-2014-0114, CVE-2019-10086, CVE-2019-10202, CVE-2019-10172, CVE-2019-17571, CVE-2019-12402, CVE-2017-3734, CVE-2019-16869, CVE-2019-17195, CVE-2017-18640, CVE-2019-0201, CVE-2014-3488, CVE-2015-2156, CVE-2015-2156, CVE-2014-0193, CVE-2017-12974, CVE-2020-5024, CVE-2020-5025, CVE-2020-4976, CVE-2020-4387, CVE-2020-4386, CVE-2020-4355, CVE-2020-4363, CVE-2020-4414, CVE-2020-4420, CVE-2020-4273, CVE-2020-4701, CVE-2020-4739) XML External Entity (XXE) Injection vulnerability (CVE-2021-20453)
Description	IBM has released a fix for IBM Db2 Warehouse to address multiple vulnerabilities found in IBM Db2. IBM WebSphere Application Server is found to be vulnerable to a XML External Entity Injection (XXE) attack when processing XML data. A successful exploitation of this vulnerability could lead an attacker to expose sensitive information or consume memory resources of an affected system.
Affected Products	IBM Db2 Warehouse all versions WebSphere Application Server version 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/6445171 https://www.ibm.com/support/pages/node/6445171

Affected Product	Red Hat
Severity	**High**
Affected Vulnerability	Nettle signature verification functionality failure(CVE-2021-20305)
Description	A flaw was found in Nettle, where several Nettle signature verification functions (GOST DSA, EDDSA & ECDSA) result in the Elliptic Curve Cryptography point (ECC) multiply function being called with out-of-range scalers, possibly resulting in incorrect results. This flaw allows an attacker to force an invalid signature, causing an assertion failure or possible validation.
Affected Products	Red Hat Enterprise Linux 7 Red Hat Enterprise Linux 8 Red Hat Enterprise Linux 8 Red Hat Enterprise Linux 8.1 Extended Update Support Red Hat Enterprise Linux 8.2 Extended Update Support
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/security/cve/CVE-2021-20305?extIdCarryOver=true&sc_cid=701f2000001OH7JAAW

Affected Product	Hewlett Packard
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities(CVE-2021-20233, CVE-2020-25632, CVE-2020-27779, CVE-2021-20225, CVE-2020-27749, CVE-2020-25647)
Description	HPE has issued security updates in response to multiple vulnerabilities found in open source GRUB2 boot loader and UEFI Forbidden Signature Database (DBX) to protect system secure boot when the secure boot feature is enabled on HPE systems. DBX updates provided by the operating system vendors will also need to be applied to acquire complete protection from malicious attacks against secure boot integrity.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04116en_us

Affected Product	WordPress
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	WordPress releases its security and maintenance update in order to address two vulnerabilities including XXE vulnerability within the media library affecting PHP 8, data exposure vulnerability within the REST API and multiple bug fixes.
Affected Products	WordPress versions prior 5.7.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://wordpress.org/news/2021/04/wordpress-5-7-1-security-and-maintenance-release/

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.