Advisory Alert

Alert Number : AAA20210326 **Date :** March 26, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Juniper	**Critical**	**Denial of Service**
Redhat	**High**	**Multiple Vulnerabilities**
Samba	**High**	**Multiple Vulnerabilities**
OpenSSL	**High**	**Multiple Vulnerabilities**
CPanel	**High**	**lead to an HTTP Request**
SolarWinds - Orion Platform	**High**	**Remote code execution**

Description

Affected Product	**Juniper**
Severity	**Critical**
Affected Vulnerability	Denial of Service (CVE-2021-0211)
Description	An improper check for unusual or exceptional conditions in Juniper Networks Junos OS with Evolved Routing Protocol service allows an attacker to send a valid BGP FlowSpec message thereby causing an unexpected changes in the routeing advertisements within the BGP FlowSpec domain leading to disruptions in network traffic causing a Denial of Service condition.
Affected Products	All versions prior to 17.3R3-S10 with the exceptions of 15.1X49-D240 on SRX Series and 15.1R7-S8 on EX Series 17.4 versions prior to 17.4R2-S12, 17.4R3-S4 18.1 versions prior to 18.1R3-S12 18.2 versions prior to 18.2R2-S8, 18.2R3-S6 18.3 versions prior to 18.3R3-S4 18.4 versions prior to 18.4R1-S8, 18.4R2-S6, 18.4R3-S6 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S3 19.2 versions prior to 19.2R3-S1 19.3 versions prior to 19.3R2-S5, 19.3R3-S1 19.4 versions prior to 19.4R1-S3, 19.4R2-S3, 19.4R3 20.1 versions prior to 20.1R2 20.2 versions prior to 20.2R1-S3 20.2R2 20.3 versions prior to 20.3R1-S1, 20.3R2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11101&cat=SIRT_1&actp=LIST

Affected Product	**Redhat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2015-8011 ,CVE-2020-14349 ,CVE-2020-14350)
Description	Redhat released security patch updates addressing Multiple vulnerabilities **CVE-2015-8011-** Buffer overflow in the lldp_decode function in daemon/protocols/lldp.c in lldpd allows remote attackers to cause a denial of service and possibly execute arbitrary code via vectors involving large management addresses and TLV boundaries **CVE-2020-14349** -PostgreSQL versions did not properly sanitize the search_path during logical replication. An authenticated attacker could use this flaw in an attack execute arbitrary SQL command in the context of the user used for replication. **CVE-2020-14350** - PostgreSQL extensions did not use search_path safely in their installation script. An attacker with sufficient privileges could use this flaw to trick an administrator into executing a specially crafted script, during the installation or update of such extension
Affected Products	Red Hat Virtualization 4 for RHEL 8 x86_64 Red Hat Virtualization Host 4 for RHEL 8 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2021:0988

Affected Product	**Samba**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-27840, CVE-2021-20277)
Description	This vulnerabilities are allows a remote attacker to execute arbitrary code and denial of service (DoS) attack on the targeted system **CVE-2020-27840** - A remote attacker can send specially crafted LDAP request to Samba AD DC LDAP server, trigger heap-based buffer overflow and execute arbitrary codes. **CVE-2021-20277** - A remote user can send a specially crafted LDAP query, trigger out-of-bounds read error and crash the LDAP server.Due to a boundary condition in ldb_handler_fold() function when processing multiple consecutive leading spaces within LDAP query.
Affected Products	All Samba versions since Samba 4.0.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.samba.org/samba/security/CVE-2020-27840.html https://www.samba.org/samba/security/CVE-2021-20277.html

Affected Product	**OpenSSL**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-3450, CVE-2021-3449)
Description	**CVE-2021-3450** - An error in the implementation of this check meant that the result of a previous check to confirm that certificates in the chain are valid CA certificates was overwritten. This effectively bypasses the check that non-CA certificates must not be able to issue other certificates. If a "purpose" has been configured then there is a subsequent opportunity for checks that the certificate is a valid CA. Where a purpose is set the certificate chain will still be rejected even when the strict flag has been used. **CVE-2021-3449** - An OpenSSL TLS server may crash if sent a maliciously crafted renegotiation ClientHello message from a client. If a TLSv1.2 renegotiation ClientHello omits the signature_algorithms extension, but includes a signature_algorithms_cert extension then a NULL pointer dereference will result, leading to a crash and a denial of service attack. A server is only vulnerable if it has TLSv1.2 and renegotiation enabled.
Affected Products	OpenSSL versions 1.1.1h and newer are affected by this issue
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.openssl.org/news/secadv/20210325.txt

Affected Product	**CPanel**
Severity	**High**
Affected Vulnerability	HTTP Request Smuggling attack. (CVE-2020-25613)
Description	This vulnerability was discovered in Ruby through WEBrick, a simple HTTP server bundled with Ruby, had not checked the transfer encoding header value correctly. An attacker may potentially exploit this issue to bypass a reverse proxy, which may lead to an HTTP Request Smuggling attack.
Affected Products	All versions of Ruby through 2.7.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://news.cpanel.com/easyapache-4-march-24-release/

Affected Product	**SolarWinds - Orion Platform**
Severity	**High**
Affected Vulnerability	Remote code execution (CVE-2021-3109, CVE-2020-35856)
Description	Solar Winds has release new update also brings a number of security improvements, with fixes for preventing XSS attacks and enabling UAC protection for Orion database manager, among others. Orion is recommended to update to the latest release to mitigate the risk associated with the security issues.
Affected Products	Previous releases of Orion Platform before 2020.2.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://documentation.solarwinds.com/en/Success_Center/orionplatform/Content/Release_Notes/Orion_Platform_2020-2-5_release_notes.htm

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.