Advisory Alert

Alert Number: AAA20211202 **Date:** December 2, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Redhat	**Critical**	Heap overflow Vulnerability

Description

Affected Product	Redhat
Severity	**Critical**
Affected Vulnerability	Heap overflow Vulnerability (CVE-2021-43527)
Description	A flaw was found in the way NSS verifies certificates. This flaw allows an attacker posing as an SSL/TLS server to trigger this issue in a client application compiled with NSS when it tries to initiate an SSL/TLS connection
Affected Products	Red Hat Enterprise Linux for x86_64 8 x86_64 Red Hat Enterprise Linux for IBM z Systems 8 s390x Red Hat Enterprise Linux for Power, little endian 8 ppc64le Red Hat Enterprise Linux for ARM 64 8 aarch64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/security/cve/CVE-2021-43527

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.