Advisory Alert

Alert Number: **AAA20211223** **Date:** **December 23, 2021**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Red Hat	**Medium**	Remote Code Execution Vulnerability

Description

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Remote Code Execution Vulnerability (CVE-2021-4104)
Description	The vulnerability exists due to insecure input validation when processing serialized data in JMSAppender, when the attacker has write access to the Log4j configuration. The attacker can provide TopicBindingName and TopicConnectionFactoryBindingName configurations causing JMSAppender to perform JNDI requests that result in remote code execution. All Red Hat users are encouraged to upgrade to the latest versions.
Affected Products	Red Hat Software Collections (for RHEL Server) 1 for RHEL 7 x86_64 Red Hat Software Collections (for RHEL Server for System Z) 1 for RHEL 7 s390x Red Hat Software Collections (for RHEL Server for IBM Power LE) 1 for RHEL 7 ppc64le Red Hat Software Collections (for RHEL Workstation) 1 for RHEL 7 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2021:5269

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.