Advisory Alert

Alert Number: AAA20230103 **Date:** January 3, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Redhat	**High**	Out-of-bounds writing vulnerability

Description

Affected Product	**Redhat**
Severity	**High**
Affected Vulnerability	Out-of-bounds writing vulnerability (CVE-2022-42920)
Description	RedHat has released a security update addressing an out-of-bounds writing vulnerability that exists in the Byte Code Engineering Library (Apache Commons BCEL) that is used in their products. **CVE-2022-42920** - Apache Commons BCEL has a number of APIs that would normally only allow changing specific class characteristics. However, due to an out-of-bounds writing issue, these APIs can be used to produce arbitrary bytecode. An attacker can abuse this to pass attacker-controllable data to those APIs, giving the attacker more control over the resulting bytecode than otherwise expected. Redhat recommends to apply the necessary patch updates at your earliest to avoid issues
Affected Products	Red Hat Enterprise Linux for x86_64 9 x86_64 Red Hat Enterprise Linux for IBM z Systems 9 s390x Red Hat Enterprise Linux for Power, little endian 9 ppc64le Red Hat Enterprise Linux for ARM 64 9 aarch64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2023:0005

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.