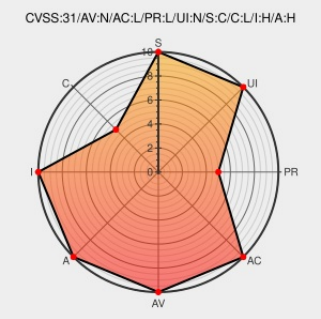
CVE-2022-21675

Published on: 01/12/2022 12:00:00 AM UTC

Last Modified on: 01/19/2022 07:25:00 PM UTC

CVE-2022-21675 - advisory for GHSA-3wq9-j4fc-4wmc

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Bytecode Viewer from Bytecode Viewer Project contain the following vulnerability:

Bytecode Viewer (BCV) is a Java/Android reverse engineering suite. Versions of the package prior to 2.11.0 are vulnerable to Arbitrary File Write via Archive Extraction (AKA "Zip Slip"). The vulnerability is exploited using a specially crafted archive that holds directory traversal filenames (e.g. ../../evil.exe). The Zip Slip vulnerability can affect numerous archive formats, including zip, jar, tar, war, cpio, apk, rar and 7z. The attacker can then overwrite executable files and either invoke them remotely or wait for the system or user to call them, thus achieving remote command execution on the victim's machine. The impact of a Zip Slip vulnerability would allow an attacker to create or overwrite existing files on the filesystem. In the context of a web application, a web shell could be placed within the application directory to achieve code execution. All users should upgrade to BCV v2.11.0 when possible to receive a patch. There are no recommended workarounds aside from upgrading.

CVE-2022-21675 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Konloch** - **bytecode-viewer** version **< 2.11.0**

CVSS3 Score: 7.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 6.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE

Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Improve Zip Slip detection · Konloch/bytecode-viewer@1ec0265 · GitHub	github.com text/html	MISC github.com/Konloch/bytecode-viewer/commit/1ec02658fe6858162f5e6a24f97928de6696c5cb
Release 2.11.0 - Security Update · Konloch/bytecode-viewer · GitHub	github.com text/html	MISC github.com/Konloch/bytecode-viewer/releases/tag/v2.11.0
Bytecode Viewer v2.10.x Zip Slip · Advisory · Konloch/bytecode-viewer · GitHub	github.com text/html	CONFIRM github.com/Konloch/bytecode-viewer/security/advisories/GHSA-3wq9-j4fc-4wmc
Mitigate Zip Slip exlpoit · Konloch/bytecode-viewer@c968e94 · GitHub	github.com text/html	MISC github.com/Konloch/bytecode-viewer/commit/c968e94b2c93da434a4ecfac6d08eda162d615d0

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Bytecode Viewer Project	Bytecode Viewer	All	All	All	All

cpe:2.3:a:bytecode_viewer_project:bytecode_viewer:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-21675 : Bytecode Viewer BCV is a Java/Android reverse engineering suite. Versions of the package prior t… twitter.com/i/web/status/1…	2022-01-12 18:26:07

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report