Security Advisory Report - OBSO-1806-03

Zip Slip (CVE-2018-8009, 2018-11771)

Creation Date: 2018-06-15 12:08:12
Last Update: 2018-10-18 15:31:01

Summary

Zip Slip is a widespread critical archive extraction vulnerability, allowing attackers to write arbitrary files on the system, typically resulting in remote command execution.
It was discovered and responsibly disclosed by the Snyk Security team ahead of a public disclosure on 5th June 2018, and affects thousands of projects, including ones from HP, Amazon, Apache, Pivotal and many more (CVEs and full list here) .

The vulnerability has been found in multiple ecosystems, including JavaScript, Ruby, .NET and Go, but is especially prevalent in Java, where there is no central library offering high level processing of archive (e.g. zip) files. The lack of such a library led to vulnerable code snippets being hand crafted and shared among developer communities such as StackOverflow .
The vulnerability is exploited using a specially crafted archive that holds directory traversal filenames (e.g. ../../evil.sh). The Zip Slip vulnerability can affect numerous archive formats, including tar, jar, war, cpio, apk, rar and 7z.

Zip Slip is a form of directory traversal that can be exploited by extracting files from an archive. The premise of the directory traversal vulnerability is that an attacker can gain access to parts of the file system outside of the target folder in which they should reside. 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 vulnerability can also cause damage by overwriting configuration files or other sensitive resources, and can be exploited on both client (user) machines and servers.

...

https://res.cloudinary.com/snyk/image/upload/v1528192501/zip-slip-vulnerability/technical-whitepaper.pdf

Details

The two parts required to exploit this vulnerability is a malicious archive and extraction code that does not perform validation checking.

First of all, the contents of the zip file needs to have one or more files that break out of the target directory when extracted.

The contents of this zip file have to be hand crafted. Archive creation tools don't typically allow users to add files with these paths, despite the zip specification allowing it. However, with the right tools, it's easy to create files with these paths.

...

The second thing you'll need to exploit this vulnerability is to extract the archive, either using your own code or a library. The vulnerability exists when the extraction code omits validation on the file paths in the archive.

Affected libraries:
https://github.com/snyk/zip-slip-vulnerability

Affected libraries used by Unify products:

Apache Hadoop CVE-2018-8009

Apache Hive CVE-2018-8009

Apache Maven
Apache Maven itself is not vulnerable, since Maven doesn't unpack by itself: unpacking actions are done by plugins.

Apache Ant
Apache Ant up to 1.9.11 has the same issue with its unzip task: it will be fixed in 1.9.12
https://maven.apache.org/security-plexus-archiver.html

Apache commons-compress no details available yet, Lucee server not relevant CVE-2018-11771

Orient DB used version is not affected.

.NET DotNetZip.Semverd no details available yet

Affected Products

Unify product typically do not process zip files from an external source which reduces priority.
Most affected libraries are not used by Unify products.

Apache Hadoop CVE-2018-8009

Circuit Operations node	Hadoop is removed in Sprint 96	V1.10.98.1

Apache Hive CVE-2018-8009

Circuit Operations node	Hadoop is removed in Sprint 96	V1.10.98.1

Maven

Circuit Common Operating System	Maven is not executed, only in the component list due to license reason

Ant

CMP is not affected
OpenScape 4000 is not affected
UC is not affected

Fault Management is not affected

Commons Compress CVE 2018-11771

Circuit Managment Node is not affected

Fault Management is not affected

Composer is in analysis, probably not affected

OrientDB

Composer does not use the affected version

DotNetZip.Semverd

no product is affected

All other products do nor use the vulnerable components.

Recommended Actions

Update to the product versions mentioned above.

References

https://res.cloudinary.com/snyk/image/upload/v1528192501/zip-slip-vulnerability/technical-whitepaper.pdf

https://github.com/snyk/zip-slip-vulnerability

https://snyk.io/research/zip-slip-vulnerability

https://maven.apache.org/security-plexus-archiver.html

Advisory: OBSO-1806-03, status: general release
Security Advisories are released as part of Unify's Vulnerability Intelligence Process. For more information see https://www.unify.com/security/advisories.

Contact and Disclaimer

OpenScape Baseline Security Office
obso@unify.com

Mies-van-der-Rohe Str. 6, D-80807 München
www.unify.com