XML External Entity (XXE) Injection

Affecting com.h2database:h2 package, versions [1.4.198,2.0.202)

HIGH

INTRODUCED: 30 OCT 2021 CVE-2021-23463 CWE-611 FIRST ADDED BY SNYK

Share

How to fix?

Upgrade `com.h2database:h2` to version 2.0.202 or higher.

Overview

com.h2database:h2 is a database engine

Affected versions of this package are vulnerable to XML External Entity (XXE) Injection via the `org.h2.jdbc.JdbcSQLXML` class object, when it receives parsed string data from `org.h2.jdbc.JdbcResultSet.getSQLXML()` method. If it executes the `getSource()` method when the parameter is `DOMSource.class` it will trigger the vulnerability.

Details

XXE Injection is a type of attack against an application that parses XML input. XML is a markup language that defines a set of rules for encoding documents in a format that is both human-readable and machine-readable. By default, many XML processors allow specification of an external entity, a URI that is dereferenced and evaluated during XML processing. When an XML document is being parsed, the parser can make a request and include the content at the specified URI inside of the XML document.

Attacks can include disclosing local files, which may contain sensitive data such as passwords or private user data, using file: schemes or relative paths in the system identifier.

For example, below is a sample XML document, containing an XML element- username.

```
<xml> <?xml version="1.0" encoding="ISO-8859-1"?> <username>John</username> </xml>
```

An external XML entity - `xxe`, is defined using a system identifier and present within a DOCTYPE header. These entities can access local or remote content. For example the below code contains an external XML entity that would fetch the content of `/etc/passwd` and display it to the user rendered by `username`.

```
<xml> <?xml version="1.0" encoding="ISO-8859-1"?> <!DOCTYPE foo [ <!ENTITY xxe SYSTEM "file:///etc/passwd" >]>
<username>&xxe;</username> </xml>
```

Other XXE Injection attacks can access local resources that may not stop returning data, possibly impacting application availability and leading to Denial of Service.

References

- GitHub Commit
- GitHub Issue
- GitHub PR

Snyk CVSS

Exploit Maturity	Proof of concept
Attack Complexity	Low
Confidentiality	HIGH
Availability	HIGH

See more

NVD 9.1 CRITICAL

Do your applications use this vulnerable package?

In a few clicks we can analyze your entire application and see what components are vulnerable in your application, and suggest you quick fixes.

Test your applications

Snyk ID	SNYK-JAVA-COMH2DATABASE-1769238
Published	31 Oct 2021
Disclosed	30 Oct 2021
Credit	threedr3am of SecCoder Security Lab

Report a new vulnerability Found a mistake?