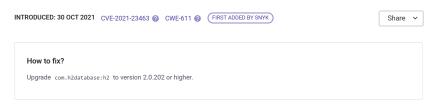
snyk Vulnerability DB

Snyk Vulnerability Database > Maven > com.h2database:h2

XML External Entity (XXE) Injection

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



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 (lass 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" >]>
```

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

PRODUCT

Snyk Open Source

Snyk Code

Snyk Container

Snyk Infrastructure as Code

Test with Github

Test with CLI

RESOURCES

Vulnerability DB

Documentation

Disclosed Vulnerabilities

Blog

FAQs

COMPANY

About



Snyk CVSS		
Exploit Maturit	y Proof of concept	0
Attack Comple	exity Low	0
Confidentiality	HIGH	9
Availability	HIGH	9
See more		
> NVD	9.1 CRITIC	AL
Do your application a few clicks	ations use this vulnerable package? we can analyze your entire application and so	
Do your application a few clicks	ations use this vulnerable package? we can analyze your entire application and sents are vulnerable in your application, and	
Do your application a few clicks what compone	ations use this vulnerable package? we can analyze your entire application and so ents are vulnerable in your application, and uick fixes.	
Do your application a few clicks what compone suggest you qu	ations use this vulnerable package? we can analyze your entire application and so ents are vulnerable in your application, and uick fixes.	ee
Do your applic In a few clicks what compone suggest you qu Test your ap	ations use this vulnerable package? we can analyze your entire application and sents are vulnerable in your application, and sick fixes. oplications	238

Report a new vulnerability Foun

Found a mistake?

Contact

Policies

Do Not Sell My Personal Information

CONTACT US

Support

Report a new vuln

Press Kit

Events

FIND US ONLINE

TRACK OUR DEVELOPMENT





© 2022 Snyk Limited

Registered in England and Wales. Company number: 09677925

Registered address: Highlands House, Basingstoke Road, Spencers Wood, Reading, Berkshire, RG7 1NT.