What's wrong with having an internet facing login page? – SQL injection in Aptean

POSTED ON 14/10/2020 BY ALEX DRABEK

Exposing administrative interfaces can be dangerous – SQL injection in Aptean

> ***TLDR;*** *We have found a time-based SQL injection in Aptean Product Configurator v4.0 SP6 – 4.61.0000 which allowed for database access.*

Have you ever wondered what are the risks of leaving a login interface exposed to the internet?

You have probably already thought of weak passwords being used, an insecure Wi-Fi during the initial connection, or the headache of giving access only to the right people. You also keep the platform up to date and patched, however this is not enough. Those are the most commonly discussed risks and they are generally well known.

When deciding to open a new page to the whole world (internet), it is important to identify the risks that are not currently known.

Conducting a penetration test is a good example for this.

During penetration testing engagement we actively try to break through current defences of the application, its platform and other internal network devices on the route.
An external penetration test starts with us discovering available attack surface and then attempting to break the systems defences with the least possible privileges.

In our test we started by examining the login page, with no further access. Our goal was to determine what could be done without authentication to the application at all.
We examined all parameters in the login page of Aptean Product Configurator v4.0 SP6 – 4.61.0000.
A GET request to /pc40/cse?
cmd=LOGIN&config_details=null&product_id=null&passTxt=LQM2PdpY&lang=null&login_type=standard&**nameTxt=** was found to be vulnerable.

```
Parameter: #1* (URI)
    Type: stacked queries
    Title: Microsoft SQL Server/Sybase stacked queries (comment)
    Payload: [redacted]/pc40/cse?cmd=LOGIN&config_details=null&
product_id=null&passTxt=LQM2PdpY&lang=null&login_type=standard&nameTxt=';WAITFOR DELA
Y '0:0:5'--
```

After numerous attempts, we found that **nameTxt** parameter was vulnerable to time-based SQL injection. This allowed for the extraction of all data stored in the application database and for further system enumeration.

This vulnerability can be exploited remotely, with no authentication.

```
back-end DBMS: Microsoft SQL Server azure
banner:
---
Microsoft SQL Server [redacted] (X64)
        [redacted]
        Copyright (c) Microsoft Corporation
        Enterprise Edition (64-bit) [redacted]
---
```

From this we uncovered previously unknown risk and helped the client with making better decisions for their business.

To conclude, it is important to do due diligence cost-effectively and attempt to uncover risks.

If you would like more information about our methods and testing, visit our testing services page or please contact us and we can arrange a scoping call or demo of our technical services.

Contact us

Discovered by Alexander Drabek

CVE number: CVE-2020-26944
Discovery 1st October 2020
Aptean informed – Acknowledgement on 19th October

Vendor is working on a patch and performing further security tasks to ensure security of their products.
Any current and past customers affected by this vulnerability are invited to reach out to Aptean Customer Support to obtain the patch and assistance applying it.

POSTED IN ARTICLE, CVE, FRONT PAGE, NEWS, SECURITY, SOFTWARE SECURITY, TESTING
TAGGED CVE, FRONT PAGE, SQL INJECTION, SQLI, VULNERABILITY

RECENT POSTS

9 Basic Steps to help check an email isn't Phishing

5 key security factors to working from home more safely

ARCHIVES

CATEGORIES