Re: [scr1162372] your CVE ID requests

Received: **Friday, March 25, 2022 2:54 PM**

From: **cve-request@mitre.org**

To: **hackermark@pm.me**

CC: **cve-request@mitre.org**

> [Suggested description]
> An SQL Injection vulnerability exists in OpenMRS Reference Application
> Standalone Edition <=2.11 and Platform Standalone Edition <=2.4.0 via
> GET requests on arbitrary parameters in patient.page.
>
> ----------
>
> [Additional Information]
> Notification and proof of concept submitted to security@openmrs.org as per responsible disclosure guidelines outlined here: https://wiki.openmrs.org/display/docs/Reporting+Bugs. Issue submitted at 10/25/2021 @ 10:37 AM ET. Report acknowledged on 11:24 AM same day. Emails available on request. Currently pending a reply from security team so I can create a JIRA ticket for further documentation.
>
> ----------
>
> [Vulnerability Type]
> SQL Injection
>
> ----------
>
> [Vendor of Product]
> OpenMRS
>
> ----------
>
> [Affected Product Code Base]
> Reference Application Standalone Edition - <=2.11
> Platform Standalone Edition - <=2.4.0
>
> ----------
>
> [Affected Component]
> /openmrs/coreapps/clinicianfacing/patient.page
>
> ----------
>
> [Attack Type]
> Local
>
> ----------

>
> [Impact Denial of Service]
> true
>
> ----------
>
> [Impact Information Disclosure]
> true
>
> ----------
>
> [CVE Impact Other]
> Theft of patient data
>
> ----------
>
> [Attack Vectors]
> Authenticated GET requests on arbitrary parameters in affected component. Attacks take the form of: /openmrs/coreapps/clinicianfacing/patient.page?patientId=###&[fake parameter]='{SQL statement]'1
>
> ----------
>
> [Reference]
> https://wiki.openmrs.org/display/docs/Reporting+Bugs
> https://openmrs.org/demo/
>
> ----------
>
> [Has vendor confirmed or acknowledged the vulnerability?]
> true
>
> ----------
>
> [Discoverer]
> Mark Rudnitsky

Use CVE-2021-43094.

> [Suggested description]
> The MetaPicz online image metadata viewer has an unauthenticated
> reflected cross-site scripting vulnerability. By modifying a certain
> parameter in "view.php", an attacker can inject and execute arbitrary
> JavaScript code.
>
> ----------
>
> [Additional Information]
> Vendor website is offline. Twitter and Facebook accounts appear to be defunct or non-existent. Sent an email following responsible disclosure guidelines to info@securo.it and inbox appears to be unmonitored. Have no way of contacting the company otherwise. No responses have been received.
>
> Exact PoC is:
> http://metapicz.com/view.php?action=metadata-get&format=html&imageUrl=https://pixy.org/src/477/4774988.jpg >

```
>
> Recommend testing with Chrome with XSS Auditor disabled. Also recommend using HTTP as
HTTPS breaks the site functionality.
>
> ----------------------------------------
>
> [Vulnerability Type]
> Cross Site Scripting (XSS)
>
> ----------------------------------------
>
> [Vendor of Product]
> Secureo.it
>
> ----------------------------------------
>
> [Affected Product Code Base]
> MetaPicz - 1.0
>
> ----------------------------------------
>
> [Affected Component]
> https://metapicz.com/view.php
>
> ----------------------------------------
>
> [Attack Type]
> Local
>
> ----------------------------------------
>
> [Impact Code execution]
> true
>
> ----------------------------------------
>
> [Impact Information Disclosure]
> true
>
> ----------------------------------------
>
> [CVE Impact Other]
> Session takeover, cookie theft, client side data manipulation, redirects to malicious
sites
>
> ----------------------------------------
>
> [Attack Vectors]
> Crafted payload in "view.php" parameter allows for injection of arbitrary Javascript.
>
> ----------------------------------------
>
> [Reference]
> https://metapicz.com
> https://securo.it
>
> ----------------------------------------
```

>
> [Discoverer]
> Mark Rudnitsky

a Hosted Service

--
CVE Assignment Team
M/S M300, 202 Burlington Road, Bedford, MA 01730 USA
 [A PGP key is available for encrypted communications at
   https://cve.mitre.org/cve/request_id.html]