

# Compliance Report

## NIST Special Publication 800-53 Revision 4 - Security and Privacy Controls for Federal Information Systems and Organizations

### Description

This publication has been developed by NIST to further its statutory responsibilities under the Federal Information Security Management Act (FISMA), Public Law (P.L.) 107-347

This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), Securing Agency Information Systems, as analyzed in Circular A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided in Circular A-130, Appendix III, Security of Federal Automated Information Resources.

This publication provides a catalog of security and privacy controls for federal information systems and organizations and a process for selecting controls to protect organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation from a diverse set of threats including hostile cyber attacks, natural disasters, structural failures, and human errors.

### Disclaimer

This document or any of its content cannot account for, or be included in any form of legal advice. The outcome of a vulnerability scan (or security evaluation) should be utilized to ensure that diligent measures are taken to lower the risk of potential exploits carried out to compromise data.

Legal advice must be supplied according to its legal context. All laws and the environments in which they are applied, are constantly changed and revised. Therefore no information provided in this document may ever be used as an alternative to a qualified legal body or representative.

This document was generated using information provided in "NIST Special Publication 800-53", that can be found at <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>.

# Compliance at a Glance

---

## CATEGORY

0	AC-3 ACCESS ENFORCEMENT
0	AC-7 UNSUCCESSFUL LOGON ATTEMPTS
0	AC-12 SESSION TERMINATION
0	AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION
20	AC-22 PUBLICLY ACCESSIBLE CONTENT
55	CM-6 CONFIGURATION SETTINGS
0	CM-7 LEAST FUNCTIONALITY
0	IA-2 USER IDENTIFICATION AND AUTHENTICATION
34	MA-2 CONTROLLED MAINTENANCE
0	SC-2 APPLICATION PARTITIONING
18	SC-4 INFORMATION IN SHARED RESOURCES
0	SC-5 DENIAL OF SERVICE PROTECTION
4	SC-8 TRANSMISSION CONFIDENTIALITY AND INTEGRITY
0	SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT
0	SC-23 SESSION AUTHENTICITY
34	SI-2 FLAW REMEDIATION
0	SI-10 INFORMATION INPUT VALIDATION
4	SI-11 ERROR HANDLING
0	SI-15 INFORMATION OUTPUT FILTERING
0	SI-16 MEMORY PROTECTION

## Detailed Compliance Report by Category

This section is a detailed report that explains each vulnerability found according to individual compliance categories.

### AC-3 ACCESS ENFORCEMENT

---

The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

**No alerts in this category**

### AC-7 UNSUCCESSFUL LOGON ATTEMPTS

---

Enforces a limit of defined number of consecutive invalid logon attempts by a user during a defined time period

**No alerts in this category**

### AC-12 SESSION TERMINATION

---

The information system automatically terminates a session after a defined time period of inactivity.

**No alerts in this category**

### AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION

---

**No alerts in this category**

### AC-22 PUBLICLY ACCESSIBLE CONTENT

---

The organization reviews the content on the publicly accessible information system for nonpublic information and removes such information, if discovered.

## Possible sensitive files

---

A possible sensitive file has been found. This file is not directly linked from the website. This check looks for common sensitive resources like password files, configuration files, log files, include files, statistics data, database dumps. Each one of these files could help an attacker to learn more about his target.

### CWE

CWE-200

### CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

### CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

## Impact

---

This file may expose sensitive information that could help a malicious user to prepare more advanced attacks.

## <http://10.10.236.31/>

Possible sensitive files:

- <http://10.10.236.31/openemr/admin.php>

## Request

---

```
GET /openemr/admin.php HTTP/1.1
Accept: ydabcrvp/kkoy
Cookie: OpenEMR=bbs8OgzIFbvo7hR%2Cj5ZvMq%2C3QTQmauASLmo3p3YX9WgoZJp2
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
```

Host: 10.10.236.31  
Connection: Keep-alive

## <http://192.168.145.128/>

Possible sensitive files:

- <http://192.168.145.128/openemr/admin.php>

### Request

---

```
GET /openemr/admin.php HTTP/1.1
Accept: shxrinco/hemy
Cookie: OpenEMR=ShqPYxeckgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

### Recommendation

---

Restrict access to this file or remove it from the website.

### References

---

#### [Web Server Security and Database Server Security](#)

<https://www.acunetix.com/websitesecurity/webserver-security/>

## Application error messages

---

This alert requires manual confirmation

Acunetix found one or more error/warning messages. Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

These messages may also contain the location of the file that produced an unhandled exception.  
Consult the 'Attack details' section for more information about the affected page(s).

### CWE

CWE-209

### CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

### CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Access Vector	Network
Access Complexity	Low

Base Score	5.3
Attack Vector	Network

Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

## Impact

---

Error messages may disclose sensitive information which can be used to escalate attacks.

### <http://10.10.236.31/>

Application error messages:

- http://10.10.236.31/openemr/interface/main/main\_screen.php  
**Unknown column 'Array' in 'where clause'**
- http://10.10.236.31/openemr/interface/main/main\_screen.php  
**<b>Warning</b>: include\_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php): failed to open stream: No such file or directory in <b>/var/www/html/openemr/interface/main/main\_screen.php</b> on line <b>5137</b><br />**
- http://10.10.236.31/openemr/interface/main/main\_screen.php  
**<b>Warning</b>: include\_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion (include\_path='/var/www/html/openemr/vendor/pear/archive\_tar:/var/www/html/openemr/vendor/pear/console\_getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear\_exception:::/usr/share/php') in <b>/var/www/html/openemr/interface/main/main\_screen.php</b> on line <b>5137</b><br />**
- http://10.10.236.31/openemr/interface/main/main\_screen.php  
**Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion**
- http://10.10.236.31/openemr/interface/main/messages/messages.php  
**<b>Warning</b>: include\_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php): failed to open stream: No such file or directory in <b>/var/www/html/openemr/interface/main/messages/messages.php</b> on line <b>5137</b><br />**
- http://10.10.236.31/openemr/interface/main/messages/messages.php  
**<b>Warning</b>: include\_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion**

```
(include_path='/var/www/html/openemr/vendor/pear/archive_tar:/var/www/html/openemr/vendor/pear/console_getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear_exception:::/usr/share/php') in  
<b>/var/www/html/openemr/interface/main/messages/messages.php</b> on line <b>5137</b><br />
```

- http://10.10.236.31/openemr/interface/main/messages/messages.php  
**Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion**
- http://10.10.236.31/openemr/library/ajax/dated\_reminders\_counter.php  
**<b>Warning</b>: include\_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php): failed to open stream: No such file or directory in**  
**<b>/var/www/html/openemr/library/ajax/dated\_reminders\_counter.php</b> on line <b>5137</b><br />**
- http://10.10.236.31/openemr/library/ajax/dated\_reminders\_counter.php  
**<b>Warning</b>: include\_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion**  
(include\_path='/var/www/html/openemr/vendor/pear/archive\_tar:/var/www/html/openemr/vendor/pear/console\_getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear\_exception:::/usr/share/php') in  
**<b>/var/www/html/openemr/library/ajax/dated\_reminders\_counter.php</b> on line <b>5137</b><br />**
- http://10.10.236.31/openemr/library/ajax/dated\_reminders\_counter.php  
**Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion**
- http://10.10.236.31/openemr/library/ajax/i18n\_generator.php  
**<b>Warning</b>: include\_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php): failed to open stream: No such file or directory in**  
**<b>/var/www/html/openemr/library/ajax/i18n\_generator.php</b> on line <b>5137</b><br />**
- http://10.10.236.31/openemr/library/ajax/i18n\_generator.php  
**<b>Warning</b>: include\_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion**  
(include\_path='/var/www/html/openemr/vendor/pear/archive\_tar:/var/www/html/openemr/vendor/pear/console\_getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear\_exception:::/usr/share/php') in  
**<b>/var/www/html/openemr/library/ajax/i18n\_generator.php</b> on line <b>5137</b><br />**
- http://10.10.236.31/openemr/library/ajax/i18n\_generator.php  
**Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion**
- http://10.10.236.31/openemr/interface/main/calendar/index.php  
**<b>Warning</b>: include\_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-**

mysqli\_log.inc.php): failed to open stream: No such file or directory in  
<b>/var/www/html/openemr/interface/main/calendar/index.php</b> on line <b>5137</b><br />

- http://10.10.236.31/openemr/interface/main/calendar/index.php  
<b>Warning</b>: include\_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion  
(include\_path='/var/www/html/openemr/vendor/pear/archive\_tar:/var/www/html/openemr/vendor/pear/console\_getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear\_exception:::/usr/share/php') in  
<b>/var/www/html/openemr/interface/main/calendar/index.php</b> on line <b>5137</b><br />
- http://10.10.236.31/openemr/interface/main/calendar/index.php  
Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion
- http://10.10.236.31/openemr/interface/login/login.php  
<b>Warning</b>: include\_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php): failed to open stream: No such file or directory in  
<b>/var/www/html/openemr/interface/login/login.php</b> on line <b>5137</b><br />
- http://10.10.236.31/openemr/interface/login/login.php  
<b>Warning</b>: include\_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion  
(include\_path='/var/www/html/openemr/vendor/pear/archive\_tar:/var/www/html/openemr/vendor/pear/console\_getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear\_exception:::/usr/share/php') in  
<b>/var/www/html/openemr/interface/login/login.php</b> on line <b>5137</b><br />
- http://10.10.236.31/openemr/interface/login/login.php  
Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion
- http://10.10.236.31/openemr/interface/main/tabs/main.php  
<b>Warning</b>: include\_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php): failed to open stream: No such file or directory in  
<b>/var/www/html/openemr/interface/main/tabs/main.php</b> on line <b>5137</b><br />
- http://10.10.236.31/openemr/interface/main/tabs/main.php  
<b>Warning</b>: include\_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion  
(include\_path='/var/www/html/openemr/vendor/pear/archive\_tar:/var/www/html/openemr/vendor/pear/console\_getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear\_exception:::/usr/share/php') in  
<b>/var/www/html/openemr/interface/main/tabs/main.php</b> on line <b>5137</b><br />

## Request

---

```
POST /openemr/interface/main/main_screen.php?auth=login&site=default HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://10.10.236.31/openemr
Cookie: OpenEMR=bbs8OgzIFbvo7hR%2Cj5ZvMq%2C3QTQmauASLmo3p3YX9WgoZJp2
Content-Length: 72
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 10.10.236.31
Connection: Keep-alive

authUser[] = 1&clearPass = 1&languageChoice = 1&new_login_session_management = 1
```

## <http://192.168.145.128/>

Application error messages:

- [http://192.168.145.128/openemr/interface/main/main\\_screen.php](http://192.168.145.128/openemr/interface/main/main_screen.php)  
**< b > Warning < /b >: include\_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php): failed to open stream: No such file or directory in < b >/var/www/html/openemr/interface/main/main\_screen.php< /b > on line < b >5137< /b >< br />**
- [http://192.168.145.128/openemr/interface/main/main\\_screen.php](http://192.168.145.128/openemr/interface/main/main_screen.php)  
**< b > Warning < /b >: include\_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion (include\_path='/var/www/html/openemr/vendor/pear/archive\_tar:/var/www/html/openemr/vendor/pear/cole\_getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear\_exception:::/usr/share/php') in < b >/var/www/html/openemr/interface/main/main\_screen.php< /b > on line < b >5137< /b >< br />**
- [http://192.168.145.128/openemr/interface/main/main\\_screen.php](http://192.168.145.128/openemr/interface/main/main_screen.php)  
**Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion**
- <http://192.168.145.128/openemr/interface/main/messages/messages.php>  
**< b > Warning < /b >: include\_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php): failed to open stream: No such file or directory in < b >/var/www/html/openemr/interface/main/messages/messages.php< /b > on line < b >5137< /b >< br />**
- <http://192.168.145.128/openemr/interface/main/messages/messages.php>  
**< b > Warning < /b >: include\_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion (include\_path='/var/www/html/openemr/vendor/pear/archive\_tar:/var/www/html/openemr/vendor/pear/cole\_getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear\_exception:::/usr/share/php') in < b >/var/www/html/openemr/interface/main/messages/messages.php< /b > on line < b >5137< /b >< br />**

ole\_getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear\_exception:::/usr/share/php') in  
<b>/var/www/html/openemr/interface/main/messages/messages.php</b> on line <b>5137</b><br />

- http://192.168.145.128/openemr/interface/main/messages/messages.php  
**Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion**
- http://192.168.145.128/openemr/library/ajax/dated\_reminders\_counter.php  
**<b>Warning</b>: include\_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php): failed to open stream: No such file or directory in  
<b>/var/www/html/openemr/library/ajax/dated\_reminders\_counter.php</b> on line <b>5137</b><br />**
- http://192.168.145.128/openemr/library/ajax/dated\_reminders\_counter.php  
**<b>Warning</b>: include\_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion  
(include\_path='/var/www/html/openemr/vendor/pear/archive\_tar:/var/www/html/openemr/vendor/pear/cole\_getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear\_exception:::/usr/share/php') in  
<b>/var/www/html/openemr/library/ajax/dated\_reminders\_counter.php</b> on line <b>5137</b><br />**
- http://192.168.145.128/openemr/library/ajax/dated\_reminders\_counter.php  
**Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion**
- http://192.168.145.128/openemr/interface/login/login.php  
**<b>Warning</b>: include\_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php): failed to open stream: No such file or directory in  
<b>/var/www/html/openemr/interface/login/login.php</b> on line <b>5137</b><br />**
- http://192.168.145.128/openemr/interface/login/login.php  
**<b>Warning</b>: include\_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion  
(include\_path='/var/www/html/openemr/vendor/pear/archive\_tar:/var/www/html/openemr/vendor/pear/cole\_getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear\_exception:::/usr/share/php') in  
<b>/var/www/html/openemr/interface/login/login.php</b> on line <b>5137</b><br />**
- http://192.168.145.128/openemr/interface/login/login.php  
**Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion**
- http://192.168.145.128/openemr/library/ajax/i18n\_generator.php  
**<b>Warning</b>: include\_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php): failed to open stream: No such file or directory in  
<b>/var/www/html/openemr/library/ajax/i18n\_generator.php</b> on line <b>5137</b><br />**

- http://192.168.145.128/openemr/library/ajax/i18n\_generator.php
 

**<Warning>**: include\_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion  
 (include\_path='/var/www/html/openemr/vendor/pear/archive\_tar:/var/www/html/openemr/vendor/pear/console\_getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear\_exception:::/usr/share/php') in  
**<var/www/html/openemr/library/ajax/i18n\_generator.php>** on line **5137**  
**<br />**
- http://192.168.145.128/openemr/library/ajax/i18n\_generator.php
 

Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion
- http://192.168.145.128/openemr/interface/login\_screen.php
 

**<Warning>**: include\_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php): failed to open stream: No such file or directory in  
**<var/www/html/openemr/interface/login\_screen.php>** on line **5137**  
**<br />**
- http://192.168.145.128/openemr/interface/login\_screen.php
 

**<Warning>**: include\_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion  
 (include\_path='/var/www/html/openemr/vendor/pear/archive\_tar:/var/www/html/openemr/vendor/pear/console\_getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear\_exception:::/usr/share/php') in  
**<var/www/html/openemr/interface/login\_screen.php>** on line **5137**  
**<br />**
- http://192.168.145.128/openemr/interface/login\_screen.php
 

Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion
- http://192.168.145.128/openemr/interface/main/dated\_reminders/dated\_reminders.php
 

**<Warning>**: include\_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php): failed to open stream: No such file or directory in  
**<var/www/html/openemr/interface/main/dated\_reminders/dated\_reminders.php>** on line **5137**  
**<br />**
- http://192.168.145.128/openemr/interface/main/dated\_reminders/dated\_reminders.php
 

**<Warning>**: include\_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion  
 (include\_path='/var/www/html/openemr/vendor/pear/archive\_tar:/var/www/html/openemr/vendor/pear/console\_getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear\_exception:::/usr/share/php') in  
**<var/www/html/openemr/interface/main/dated\_reminders/dated\_reminders.php>** on line **5137**  
**<br />**

- [http://192.168.145.128/openemr/interface/main/dated\\_reminders/dated\\_reminders.php](http://192.168.145.128/openemr/interface/main/dated_reminders/dated_reminders.php)  
**Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion**

## Request

---

```
GET /openemr/interface/main/main_screen.php HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: filelist;packages;aspectalerts;routes
Referer: http://192.168.145.128/openemr
Cookie: OpenEMR=fLVw-dnCSU123MMDJ4XDEMokIFFZN%2CUpmA0oNxhYR1Fnqazp
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

## Recommendation

---

Verify that these page(s) are disclosing error or warning messages and properly configure the application to log errors to a file instead of displaying the error to the user.

## Description

---

While information disclosure vulnerabilities are not directly exploitable by an attacker, they may help an attacker to learn about system specific information. The following is a list of **some** of the information an attacker may be able to obtain from application error disclosure.

- Internal IP addresses
- Secrets (passwords, keys, tokens...)
- Operating system distributions
- Software version numbers
- Missing security patches
- Application stack traces
- SQL statements
- Location of sensitive files (backups, temporary files...)
- Location of sensitive resources (databases, caches, code repositories...)

## References

---

### [PHP Runtime Configuration](#)

<https://www.php.net/manual/en/errorfunc.configuration.php#ini.display-errors>

### [Improper Error Handling](#)

[https://www.owasp.org/index.php/Improper\\_Error\\_Handling](https://www.owasp.org/index.php/Improper_Error_Handling)

# Development configuration files

---

One or more configuration files (e.g. Vagrantfile, Gemfile, Rakefile, ...) were found. These files may expose sensitive information that could help a malicious user to prepare more advanced attacks. It's recommended to remove or restrict access to this type of files from production systems.

## CWE

CWE-538

## CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

## CVSS3

CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N

Base Score	3.1
Attack Vector	Network
Attack Complexity	High
Privileges Required	None
User Interaction	Required
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

## Impact

---

These files may disclose sensitive information. This information can be used to launch further attacks.

## <http://10.10.236.31/>

Development configuration files:

- <http://10.10.236.31/openemr/package.json>

package.json => Grunt configuration file. Grunt is a JavaScript task runner.

- <http://10.10.236.31/openemr/composer.json>

composer.json => Composer configuration file. Composer is a dependency manager for PHP.

- <http://10.10.236.31/openemr/composer.lock>

composer.lock => Composer lock file. Composer is a dependency manager for PHP.

- <http://10.10.236.31/openemr/package-lock.json>

package-lock.json => npm file. This file keeps track of the exact version of every package that is installed.

- <http://10.10.236.31/openemr/public/assets/knockout/package.json>

package.json => Grunt configuration file. Grunt is a JavaScript task runner.

## Request

---

```
GET /openemr/package.json HTTP/1.1
Cookie: OpenEMR=bbs8OgzIFbvo7hR%2Cj5ZvMq%2C3QTQmauASLmo3p3YX9WgoZJp2
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 10.10.236.31
Connection: Keep-alive
```

## <http://192.168.145.128/>

Development configuration files:

- <http://192.168.145.128/openemr/package.json>

package.json => Grunt configuration file. Grunt is a JavaScript task runner.

- <http://192.168.145.128/openemr/composer.json>

composer.json => Composer configuration file. Composer is a dependency manager for PHP.

- <http://192.168.145.128/openemr/composer.lock>

composer.lock => Composer lock file. Composer is a dependency manager for PHP.

- <http://192.168.145.128/openemr/package-lock.json>

package-lock.json => npm file. This file keeps track of the exact version of every package that is installed.

- <http://192.168.145.128/openemr/public/assets/jquery-datetimepicker/package.json>

package.json => Grunt configuration file. Grunt is a JavaScript task runner.

- <http://192.168.145.128/openemr/public/assets/jquery-datetimepicker/bower.json>

bower.json => Bower manifest file. Bower is a package manager for the web.

## Request

```
GET /openemr/package.json HTTP/1.1
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

## Recommendation

Remove or restrict access to all configuration files accessible from internet.

## Directory listings

Directory listing is a web server function that displays the directory contents when there is no index file in a specific website directory. It is dangerous to leave this function turned on for the web server because it leads to information disclosure.

### CWE

CWE-538

### CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

### CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

## Impact

A user can view a list of all files from the affected directories possibly exposing sensitive information.

<http://10.10.236.31/>

Verified

Folders with directory listing enabled:

- http://10.10.236.31/openemr/interface/
- http://10.10.236.31/openemr/interface/login/
- http://10.10.236.31/openemr/public/assets/moment/min/
- http://10.10.236.31/openemr/public/assets/knockout/build/output/
- http://10.10.236.31/openemr/public/
- http://10.10.236.31/openemr/interface/main/
- http://10.10.236.31/openemr/public/assets/i18next/dist/umd/
- http://10.10.236.31/openemr/public/assets/knockout/
- http://10.10.236.31/openemr/public/assets/knockout/build/
- http://10.10.236.31/openemr/library/js/
- http://10.10.236.31/openemr/Documentation/
- http://10.10.236.31/openemr/Documentation/help\_files/
- http://10.10.236.31/openemr/public/assets/hotkeys-js/
- http://10.10.236.31/openemr/public/assets/hotkeys-js/dist/
- http://10.10.236.31/openemr/library/js/vendors/
- http://10.10.236.31/openemr/library/js/vendors/validate/
- http://10.10.236.31/openemr/public/assets/jquery-datetimepicker/build/
- http://10.10.236.31/openemr/interface/main/messages/css/
- http://10.10.236.31/openemr/public/assets/jquery/
- http://10.10.236.31/openemr/interface/main/dated\_reminders/
- http://10.10.236.31/openemr/interface/product\_registration/

## Request

---

```
GET /openemr/interface/ HTTP/1.1
Cookie: OpenEMR=bbs80gzIFbvo7hR%2Cj5ZvMq%2C3QTQmauASLmo3p3YX9WgoZJp2
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 10.10.236.31
Connection: Keep-alive
```

## <http://192.168.145.128/>

Verified

Folders with directory listing enabled:

- http://192.168.145.128/openemr/interface/
- http://192.168.145.128/openemr/interface/login/
- http://192.168.145.128/openemr/interface/main/messages/css/
- http://192.168.145.128/openemr/public/assets/
- http://192.168.145.128/openemr/public/assets/bootstrap/dist/js/
- http://192.168.145.128/openemr/interface/main/messages/js/
- http://192.168.145.128/openemr/public/assets/moment/

- <http://192.168.145.128/openemr/library/ajax/>
- [http://192.168.145.128/openemr/interface/main/dated\\_reminders/](http://192.168.145.128/openemr/interface/main/dated_reminders/)
- <http://192.168.145.128/openemr/public/assets/select2/dist/css/>
- <http://192.168.145.128/openemr/public/assets/moment/min/>
- [http://192.168.145.128/openemr/interface/product\\_registration/](http://192.168.145.128/openemr/interface/product_registration/)
- <http://192.168.145.128/openemr/Documentation/>
- <http://192.168.145.128/openemr/public/assets/bootstrap/dist/>
- <http://192.168.145.128/openemr/interface/main/tabs/js/>
- <http://192.168.145.128/openemr/public/assets/i18next/dist/>
- <http://192.168.145.128/openemr/public/assets/i18next/dist/umd/>
- <http://192.168.145.128/openemr/public/>
- <http://192.168.145.128/openemr/public/assets/i18next/>
- <http://192.168.145.128/openemr/public/assets/knockout/>
- <http://192.168.145.128/openemr/public/assets/hotkeys-js/dist/>

## Request

---

```
GET /openemr/interface/ HTTP/1.1
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

## Recommendation

---

You should make sure no sensitive information is disclosed or you may want to restrict directory listings from the web server configuration.

## Description

---

### How to disable directory listings

The easiest way to disable directory listing is to create an index file. The name of the index file depends on the web server configuration. On Apache is called index.htm, index.html. On IIS is named default.asp, default.aspx, default.htm.

On IIS directory listings are disabled by default.

For Apache you need to edit the Apache configuration file (usually named httpd.conf) or create an .htaccess file. In the configuration file you will have the definition of the directory. Something like

```
<Directory /directoryname/subdirectory> Options Indexes FollowSymLinks ...
</Directory>
```

To disable directory listing for that directory you need to remove the 'Indexes' option.

## References

---

## CWE-548: Exposure of Information Through Directory Listing

<https://cwe.mitre.org/data/definitions/548.html>

## Documentation files

One or more documentation files (e.g. `readme.txt`, `changelog.txt`, ...) were found. The information contained in these files could help an attacker identify the web application you are using and sometimes the version of the application. It's recommended to remove these files from production systems.

### CWE

CWE-538

### CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

### CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

## Impact

These files may disclose sensitive information. This information can be used to launch further attacks.

## <http://10.10.236.31/>

Documentation files:

- <http://10.10.236.31/openemr/README.md>  
File contents (first 100 characters):

```
! [Syntax Status] (https://github.com/openemr/openemr/workflows/Syntax/badge.svg?branch=rel-700)
! [Sty ...
```

- <http://10.10.236.31/openemr/interface/README.md>  
File contents (first 100 characters):

```
# OpenEMR-interface

The OpenEMR UI is built with [SASS] (https://sass-lang.com/) on top of a bootstr
...
• http://10.10.236.31/openemr/public/assets/knockout/README.md
```

File contents (first 100 characters):

```
# Knockout

**Knockout** is a JavaScript [MVVM]
(http://en.wikipedia.org/wiki/Model\_View\_ViewModel) ...
```

## Request

---

```
GET /openemr/README.md HTTP/1.1
Cookie: OpenEMR=bbs8OgzIFbvo7hR%2Cj5ZvMq%2C3QTQmauASLmo3p3YX9WgoZJp2
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 10.10.236.31
Connection: Keep-alive
```

## <http://192.168.145.128/>

Documentation files:

- <http://192.168.145.128/openemr/README.md>

File contents (first 100 characters):

```
! [Syntax Status] (https://github.com/openemr/openemr/workflows/Syntax/badge.svg?branch=rel-700)
! [Sty ...
```

- <http://192.168.145.128/openemr/interface/README.md>

File contents (first 100 characters):

```
# OpenEMR-interface
```

```
The OpenEMR UI is built with [SASS] (https://sass-lang.com/) on top of a bootstr
...

```

- <http://192.168.145.128/openemr/public/assets/jquery-datetimepicker/README.md>

File contents (first 100 characters):

```
# jQuery DateTimePicker
[Demo and Documentation] (https://xdsoft.net/jqplugins/datetimepicker/)
```

[ ! [B ...

## Request

```
GET /openemr/README.md HTTP/1.1
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

## Recommendation

Remove or restrict access to all documentation file accessible from internet.

## Possible sensitive directories

One or more possibly sensitive directories were found. These resources are not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

### CWE

CWE-200

### CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

### CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

## Impact

These directories may expose sensitive information that could help a malicious user to prepare more advanced attacks.

## <http://10.10.236.31/>

Possible sensitive directories:

- http://10.10.236.31/openemr/bin
- http://10.10.236.31/openemr/sql
- http://10.10.236.31/openemr/config
- http://10.10.236.31/openemr/tests
- http://10.10.236.31/openemr/src

### Request

---

```
GET /openemr/bin/ HTTP/1.1
Cookie: OpenEMR=bbs8OgzIFbvo7hR%2Cj5ZvMq%2C3QTQmauASLmo3p3YX9WgoZJp2
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 10.10.236.31
Connection: Keep-alive
```

## <http://192.168.145.128/>

Possible sensitive directories:

- http://192.168.145.128/openemr/bin
- http://192.168.145.128/openemr/sql
- http://192.168.145.128/openemr/config
- http://192.168.145.128/openemr/tests
- http://192.168.145.128/openemr/src

### Request

---

```
GET /openemr/bin/ HTTP/1.1
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

## Recommendation

---

Restrict access to these directories or remove them from the website.

## References

---

### [Web Server Security and Database Server Security](#)

<https://www.acunetix.com/websitemanagement/webserver-security/>

## Email addresses

---

One or more email addresses have been found on this website. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

### CWE

CWE-200

### CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

### CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	None
Integrity Impact	None
Availability Impact	None

## Impact

---

Email addresses posted on Web sites may attract spam.

### <http://10.10.236.31/>

Emails found:

- [http://10.10.236.31/openemr/acknowledge\\_license\\_cert.html](http://10.10.236.31/openemr/acknowledge_license_cert.html)  
[ajabour@iupui.edu](mailto:ajabour@iupui.edu)
- [http://10.10.236.31/openemr/acknowledge\\_license\\_cert.html](http://10.10.236.31/openemr/acknowledge_license_cert.html)  
[andres@paglayan.com](mailto:andres@paglayan.com)

- http://10.10.236.31/openemr/acknowledge\_license\_cert.html  
**superarnab@gmail.com**
- http://10.10.236.31/openemr/acknowledge\_license\_cert.html  
**drbowen@bowenmd.com**
- http://10.10.236.31/openemr/acknowledge\_license\_cert.html  
**bss@iguanasuicide.net**
- http://10.10.236.31/openemr/acknowledge\_license\_cert.html  
**brady.g.miller@gmail.com**
- http://10.10.236.31/openemr/acknowledge\_license\_cert.html  
**pandi.param@capminds.com**
- http://10.10.236.31/openemr/acknowledge\_license\_cert.html  
**stephen.waite@cmsvt.com**
- http://10.10.236.31/openemr/acknowledge\_license\_cert.html  
**amit@comlinkinc.com**
- http://10.10.236.31/openemr/acknowledge\_license\_cert.html  
**sbhayani@communitybehavioralhealth.net**
- http://10.10.236.31/openemr/acknowledge\_license\_cert.html  
**ramesh@ensoftek.com**
- http://10.10.236.31/openemr/acknowledge\_license\_cert.html  
**george.tye@gmail.com**
- http://10.10.236.31/openemr/acknowledge\_license\_cert.html  
**stone@annashaegrp.com**
- http://10.10.236.31/openemr/acknowledge\_license\_cert.html  
**fndtn357@gmail.com**
- http://10.10.236.31/openemr/acknowledge\_license\_cert.html  
**sherwin@affordablecustomehr.com**
- http://10.10.236.31/openemr/acknowledge\_license\_cert.html  
**julia.longtin@gmail.com**
- http://10.10.236.31/openemr/acknowledge\_license\_cert.html  
**ptspohnpei@gmail.com**
- http://10.10.236.31/openemr/acknowledge\_license\_cert.html  
**kevin.y@integralemr.com**
- http://10.10.236.31/openemr/acknowledge\_license\_cert.html  
**openemr@lillysystems.com**
- http://10.10.236.31/openemr/acknowledge\_license\_cert.html  
**mscltd@earthlink.net**
- http://10.10.236.31/openemr/acknowledge\_license\_cert.html  
**mdsupport@users.sf.net**

## Request

---

```
GET /openemr/acknowledge_license_cert.html HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 8595e182db21cbbc10c83c2c4cf193d3
Acunetix-Aspect-ScanID: 816589585389164376
Acunetix-Aspect-Queries: packages;aspectalerts;routes
Referer: http://10.10.236.31/openemr/interface/login/login.php
```

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
Accept-Encoding: gzip,deflate,br  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)  
Chrome/109.0.0.0 Safari/537.36  
Host: 10.10.236.31  
Connection: Keep-alive

## <http://192.168.145.128/>

Emails found:

- [http://192.168.145.128/openemr/acknowledge\\_license\\_cert.html](http://192.168.145.128/openemr/acknowledge_license_cert.html)  
**ajabour@iupui.edu**
- [http://192.168.145.128/openemr/acknowledge\\_license\\_cert.html](http://192.168.145.128/openemr/acknowledge_license_cert.html)  
**andres@paglayan.com**
- [http://192.168.145.128/openemr/acknowledge\\_license\\_cert.html](http://192.168.145.128/openemr/acknowledge_license_cert.html)  
**superarnab@gmail.com**
- [http://192.168.145.128/openemr/acknowledge\\_license\\_cert.html](http://192.168.145.128/openemr/acknowledge_license_cert.html)  
**drbowen@bowenmd.com**
- [http://192.168.145.128/openemr/acknowledge\\_license\\_cert.html](http://192.168.145.128/openemr/acknowledge_license_cert.html)  
**bss@iguanasuicide.net**
- [http://192.168.145.128/openemr/acknowledge\\_license\\_cert.html](http://192.168.145.128/openemr/acknowledge_license_cert.html)  
**brady.g.miller@gmail.com**
- [http://192.168.145.128/openemr/acknowledge\\_license\\_cert.html](http://192.168.145.128/openemr/acknowledge_license_cert.html)  
**pandi.param@capminds.com**
- [http://192.168.145.128/openemr/acknowledge\\_license\\_cert.html](http://192.168.145.128/openemr/acknowledge_license_cert.html)  
**stephen.waite@cmsvt.com**
- [http://192.168.145.128/openemr/acknowledge\\_license\\_cert.html](http://192.168.145.128/openemr/acknowledge_license_cert.html)  
**amit@comlinkinc.com**
- [http://192.168.145.128/openemr/acknowledge\\_license\\_cert.html](http://192.168.145.128/openemr/acknowledge_license_cert.html)  
**sbhayani@communitybehavioralhealth.net**
- [http://192.168.145.128/openemr/acknowledge\\_license\\_cert.html](http://192.168.145.128/openemr/acknowledge_license_cert.html)  
**ramesh@ensoftek.com**
- [http://192.168.145.128/openemr/acknowledge\\_license\\_cert.html](http://192.168.145.128/openemr/acknowledge_license_cert.html)  
**george.tye@gmail.com**
- [http://192.168.145.128/openemr/acknowledge\\_license\\_cert.html](http://192.168.145.128/openemr/acknowledge_license_cert.html)  
**stone@annashaegrp.com**
- [http://192.168.145.128/openemr/acknowledge\\_license\\_cert.html](http://192.168.145.128/openemr/acknowledge_license_cert.html)  
**fndtn357@gmail.com**
- [http://192.168.145.128/openemr/acknowledge\\_license\\_cert.html](http://192.168.145.128/openemr/acknowledge_license_cert.html)  
**sherwin@affordablecustomehr.com**
- [http://192.168.145.128/openemr/acknowledge\\_license\\_cert.html](http://192.168.145.128/openemr/acknowledge_license_cert.html)  
**julia.longtin@gmail.com**
- [http://192.168.145.128/openemr/acknowledge\\_license\\_cert.html](http://192.168.145.128/openemr/acknowledge_license_cert.html)  
**ptspohnpei@gmail.com**
- [http://192.168.145.128/openemr/acknowledge\\_license\\_cert.html](http://192.168.145.128/openemr/acknowledge_license_cert.html)  
**kevin.y@integralemr.com**

- http://192.168.145.128/openemr/acknowledge\_license\_cert.html  
openemr@lillysystems.com
- http://192.168.145.128/openemr/acknowledge\_license\_cert.html  
mscltd@earthlink.net
- http://192.168.145.128/openemr/acknowledge\_license\_cert.html  
mdsupport@users.sf.net

## Request

---

```
GET /openemr/acknowledge_license_cert.html HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/interface/login/login.php
Cookie: OpenEMR=F-6X1PVs1YyH8tue182CU%2CjzXjI%2C2Xj1wHpg%2CMTJEHOAPWa5
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

## Recommendation

---

Check references for details on how to solve this problem.

## References

---

### [Anti-spam techniques](#)

[https://en.wikipedia.org/wiki/Anti-spam\\_techniques](https://en.wikipedia.org/wiki/Anti-spam_techniques)

## Error page web server version disclosure

---

Application errors or warning messages may disclose sensitive information about an application's internal workings to an attacker.

Acunetix found the web server version number and a list of modules enabled on the target server. Consult the 'Attack details' section for more information about the affected page.

### CWE

CWE-200

### CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

### CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Access Vector	Network
---------------	---------

Base Score	5.3
------------	-----

Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

## Impact

---

Error messages information about an application's internal workings may be used to escalate attacks.

### <http://10.10.236.31/>

#### Request

---

```
GET /KnNz3PhQmq HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 10.10.236.31
Connection: Keep-alive
```

### <http://192.168.145.128/>

#### Request

---

```
GET /OSEbyESLkq HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

## Recommendation

---

Properly configure the web server not to disclose information about an application's internal workings to the user. Consult the 'Web references' section for more information.

## References

---

### [Custom Error Responses \(Apache HTTP Server\)](#)

<https://httpd.apache.org/docs/current/custom-error.html>

### [server\\_tokens \(Nginx\)](#)

[http://nginx.org/en/docs/http/ngx\\_http\\_core\\_module.html#server\\_tokens](http://nginx.org/en/docs/http/ngx_http_core_module.html#server_tokens)

### [Remove Unwanted HTTP Response Headers \(Microsoft IIS\)](#)

<https://blogs.msdn.microsoft.com/varunm/2013/04/23/remove-unwanted-http-response-headers/>

## Possible server path disclosure (Unix)

---

One or more fully qualified path names were found. From this information the attacker may learn the file system structure from the web server. This information can be used to conduct further attacks.

This alert may be a false positive, manual confirmation is required.

### CWE

CWE-200

### CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

### CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

## Impact

---

Possible sensitive information disclosure.

### <http://10.10.236.31/>

Pages with paths being disclosed:

- http://10.10.236.31/openemr/interface/main/main\_screen.php  
(/var/www/html/openemr/vendor/adodb/adodb)
- http://10.10.236.31/openemr/interface/main/messages/messages.php  
(/var/www/html/openemr/vendor/adodb/adodb)
- http://10.10.236.31/openemr/library/ajax/dated\_reminders\_counter.php  
(/var/www/html/openemr/vendor/adodb/adodb)
- http://10.10.236.31/openemr/library/ajax/i18n\_generator.php  
(/var/www/html/openemr/vendor/adodb/adodb)
- http://10.10.236.31/  
    >/var/www/html/index.html
- http://10.10.236.31/openemr/interface/main/calendar/index.php  
(/var/www/html/openemr/vendor/adodb/adodb)
- http://10.10.236.31/openemr/interface/login/login.php  
(/var/www/html/openemr/vendor/adodb/adodb)
- http://10.10.236.31/openemr/interface/main/tabs/main.php  
(/var/www/html/openemr/vendor/adodb/adodb)
- http://10.10.236.31/openemr/interface/main/dated\_reminders/dated\_reminders.php  
(/var/www/html/openemr/vendor/adodb/adodb)
- http://10.10.236.31/openemr/portal/  
    (/var/www/html/openemr/vendor/adodb/adodb)
- http://10.10.236.31/openemr/Documentation/Readme\_edihistory.html  
    /var/www/htdocs/openemr/sites/
- http://10.10.236.31/openemr/portal/messaging/secure\_chat.php  
    (/var/www/html/openemr/vendor/adodb/adodb)
- http://10.10.236.31/openemr/Documentation/help\_files/adminacl\_help.php  
    (/var/www/html/openemr/vendor/adodb/adodb)
- http://10.10.236.31/openemr/Documentation/README-Log-Backup.txt  
    /var/www/openemr
- http://10.10.236.31/openemr/Documentation/help\_files/cms\_1500\_help.php  
    (/var/www/html/openemr/vendor/adodb/adodb)
- http://10.10.236.31/openemr/Documentation/help\_files/configure\_orders\_help.php  
    (/var/www/html/openemr/vendor/adodb/adodb)
- http://10.10.236.31/openemr/library/ajax/imm\_autocomplete/search.php  
    (/var/www/html/openemr/vendor/adodb/adodb)
- http://10.10.236.31/openemr/Documentation/help\_files/mfa\_help.php  
    (/var/www/html/openemr/vendor/adodb/adodb)
- http://10.10.236.31/openemr/library/ajax/document\_helpers.php  
    (/var/www/html/openemr/vendor/adodb/adodb)
- http://10.10.236.31/openemr/interface/login\_screen.php  
    (/var/www/html/openemr/vendor/adodb/adodb)
- http://10.10.236.31/openemr/Documentation/help\_files/openemr\_installation\_help.php  
    /var/www/html/openemr

## Request

---

```
GET /openemr/interface/main/main_screen.php HTTP/1.1
Acunetix-Aspect: enabled
```

Acunetix-Aspect-Password: 8595e182db21cbbc10c83c2c4cf193d3  
Acunetix-Aspect-ScanID: 816589585389164376  
Acunetix-Aspect-Queries: filelist;packages;aspectalerts;routes  
Referer: http://10.10.236.31/openemr  
Cookie: OpenEMR=Dj68HNoGw-vYWT2k81NHDiqIHhLtRgfoVY0Tqo%2Cj6JeJm5aU  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
Accept-Encoding: gzip,deflate,br  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)  
Chrome/109.0.0.0 Safari/537.36  
Host: 10.10.236.31  
Connection: Keep-alive

## <http://192.168.145.128/>

Pages with paths being disclosed:

- [http://192.168.145.128/openemr/interface/main/main\\_screen.php](http://192.168.145.128/openemr/interface/main/main_screen.php)  
(/var/www/html/openemr/vendor/adodb/adodb)
- <http://192.168.145.128/openemr/interface/main/messages/messages.php>  
(/var/www/html/openemr/vendor/adodb/adodb)
- [http://192.168.145.128/openemr/library/ajax/dated\\_reminders\\_counter.php](http://192.168.145.128/openemr/library/ajax/dated_reminders_counter.php)  
(/var/www/html/openemr/vendor/adodb/adodb)
- <http://192.168.145.128/openemr/interface/login/login.php>  
(/var/www/html/openemr/vendor/adodb/adodb)
- [http://192.168.145.128/openemr/library/ajax/i18n\\_generator.php](http://192.168.145.128/openemr/library/ajax/i18n_generator.php)  
(/var/www/html/openemr/vendor/adodb/adodb)
- <http://192.168.145.128/>  
>/var/www/html/index.html
- [http://192.168.145.128/openemr/interface/login\\_screen.php](http://192.168.145.128/openemr/interface/login_screen.php)  
(/var/www/html/openemr/vendor/adodb/adodb)
- [http://192.168.145.128/openemr/interface/main/dated\\_reminders/dated\\_reminders.php](http://192.168.145.128/openemr/interface/main/dated_reminders/dated_reminders.php)  
(/var/www/html/openemr/vendor/adodb/adodb)
- <http://192.168.145.128/openemr/interface/main/tabs/main.php>  
(/var/www/html/openemr/vendor/adodb/adodb)
- <http://192.168.145.128/openemr/interface/portal/>  
(/var/www/html/openemr/vendor/adodb/adodb)
- <http://192.168.145.128/openemr/portal/messaging/messages.php>  
(/var/www/html/openemr/vendor/adodb/adodb)
- [http://192.168.145.128/openemr/portal/messaging/secure\\_chat.php](http://192.168.145.128/openemr/portal/messaging/secure_chat.php)  
(/var/www/html/openemr/vendor/adodb/adodb)
- [http://192.168.145.128/openemr/Documentation/Readme\\_edihistory.html](http://192.168.145.128/openemr/Documentation/Readme_edihistory.html)  
/var/www/htdocs/openemr/sites/
- [http://192.168.145.128/openemr/Documentation/help\\_files/add\\_edit\\_transactions\\_dashboard\\_help.php](http://192.168.145.128/openemr/Documentation/help_files/add_edit_transactions_dashboard_help.php)  
(/var/www/html/openemr/vendor/adodb/adodb)
- <http://192.168.145.128/openemr/Documentation/README-Log-Backup.txt>  
/var/www/openemr

- http://192.168.145.128/openemr/Documentation/help\_files/adminacl\_help.php  
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/Documentation/help\_files/cms\_1500\_help.php  
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/library/FeeSheet.class.php  
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/Documentation/help\_files/common\_help.php  
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/library/FeeSheetHtml.class.php  
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/Documentation/help\_files/configure\_orders\_help.php  
(/var/www/html/openemr/vendor/adodb/adodb)

## Request

---

```
GET /openemr/interface/main/main_screen.php HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: filelist;packages;aspectalerts;routes
Referer: http://192.168.145.128/openemr
Cookie: OpenEMR=fLVw-dnCSU123MMDJ4XDEmokIFFZN%2CUpmA0oNxhYR1Fnqazp
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

## Recommendation

---

Prevent this information from being displayed to the user.

## References

---

### [Full Path Disclosure](#)

[https://www.owasp.org/index.php/Full\\_Path\\_Disclosure](https://www.owasp.org/index.php/Full_Path_Disclosure)

## Composer installed.json publicly accessible

---

A **installed.json** file was discovered. Composer is a tool for dependency management in PHP. It allows you to declare the libraries your project depends on and it will manage (install/update) them for you. After installing the dependencies, Composer stores the list of them in a special file for internal purposes.

As the file is publicly accessible, it leads to disclosure of information about components used by the web application.

## CWE

CWE-200

## CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

## CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N

Base Score	5.8
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Changed
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

## Impact

installed.json discloses sensitive information. This information can be used to launch further attacks.

## <http://10.10.236.31/openemr/vendor/>

### Request

```
GET /openemr/vendor/composer/installed.json HTTP/1.1
Cookie: OpenEMR=t8OBjqR%2C0IVS5N1iDb%2CWppNgQ0K3h5UOCm1n0u5jQeS8WoRL
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 10.10.236.31
Connection: Keep-alive
```

## <http://192.168.145.128/openemr/vendor/>

### Request

```
GET /openemr/vendor/composer/installed.json HTTP/1.1
Cookie: OpenEMR=F-6X1PVs1YyH8tuel82CU%2CjzXjI%2C2Xj1wHpg%2CMTJEHOAPWa5
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
```

## Recommendation

---

Restrict access to vendors directory

## References

---

### [Composer Basic usage](#)

<https://getcomposer.org/doc/01-basic-usage.md>

# CM-6 CONFIGURATION SETTINGS

---

The organization configures the security settings of information technology products to the most restrictive mode consistent with information system operational requirements.

## Vulnerable package dependencies [high]

---

One or more packages that are used in your web application are affected by known vulnerabilities. Please consult the details section for more information about each affected package.

### CWE

CWE-1104

## Impact

---

The impact of this vulnerability is different for each vulnerable package. It's recommended to investigate each vulnerable package individually.

### <http://10.10.236.31/openemr/>

List of vulnerable **composer** packages:

**Package:** dompdf/dompdf

**Version:** 1.2.2

**CVE:** CVE-2022-41343

**Title:** Files or Directories Accessible to External Parties

**Description:** registerFont in FontMetrics.php in Dompdf before 2.0.1 allows remote file inclusion because a URI validation failure does not halt font registration, as demonstrated by a @font-face rule.

**CVSS V2:**

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

**CWE:** CWE-552

**References:**

- <https://github.com/dompdf/dompdf/releases/tag/v2.0.1>
- <https://github.com/dompdf/dompdf/issues/2994>
- <https://github.com/dompdf/dompdf/pull/2995>
- <https://tantosec.com/blog/cve-2022-41343/>

**Package:** dompdf/dompdf

**Version:** 1.2.2

**CVE:** CVE-2023-23924

**Title:** Incorrect Authorization

**Description:** Dompdf is an HTML to PDF converter. The URI validation on dompdf 2.0.1 can be bypassed on SVG parsing by passing `<image>` tags with uppercase letters. This may lead to arbitrary object unserialize on PHP < 8, through the `phar` URL wrapper. An attacker can exploit the vulnerability to call arbitrary URL with arbitrary protocols, if they can provide a SVG file to dompdf. In PHP versions before 8.0.0, it leads to arbitrary unserialize, that will lead to the very least to an arbitrary file deletion and even remote code execution, depending on classes that are available.

**CVSS V2:**

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

**CWE:** CWE-863

**References:**

- <https://github.com/dompdf/dompdf/security/advisories/GHSA-3cw5-7cxw-v5qg>
- <https://github.com/dompdf/dompdf/releases/tag/v2.0.2>
- <https://github.com/dompdf/dompdf/commit/7558f07f693b2ac3266089f21051e6b78c6a0c85>

**Package:** dompdf/dompdf

**Version:** 1.2.2

**CVE:** CVE-2023-24813

**Title:** Interpretation Conflict

**Description:** Dompdf is an HTML to PDF converter written in php. Due to the difference in the attribute parser of Dompdf and php-svg-lib, an attacker can still call arbitrary URLs with arbitrary protocols. Dompdf parses the href attribute of `image` tags and respects `xlink:href` even if `href` is specified. However, php-svg-lib, which is later used to parse the svg file, parses the href attribute. Since `href` is respected if both `xlink:href` and `href` is specified, it's possible to bypass the protection on the Dompdf side by providing an empty `xlink:href` attribute. An attacker can exploit the vulnerability to call arbitrary URLs with arbitrary protocols if they provide an SVG file to the Dompdf. In PHP versions before 8.0.0, it leads to arbitrary unserialize, which will lead, at the very least, to arbitrary file deletion and might lead to remote code execution, depending on available classes. This vulnerability has been addressed in commit `95009ea98` which has been included in release version 2.0.3. Users are advised to upgrade. There are no known workarounds for this vulnerability.

**CVSS V2:**

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

**CWE:** CWE-436

**References:**

- <https://github.com/dompdf/dompdf/security/advisories/GHSA-56gj-mvh6-rp75>
- <https://github.com/dompdf/dompdf/commit/95009ea98230f9b084b040c34e3869ef3dccc9aa>

**Package:** guzzlehttp/guzzle

**Version:** 7.4.4

**CVE:** CVE-2022-31091

**Title:**

**Description:** Guzzle, an extensible PHP HTTP client. `Authorization` and `Cookie` headers on requests are sensitive information. In affected versions on making a request which responds with a redirect to a URI with a different port, if we choose to follow it, we should remove the `Authorization` and `Cookie` headers from the request, before continuing. Previously, we would only consider a change in host or scheme. Affected Guzzle 7 users should upgrade to Guzzle 7.4.5 as soon as possible. Affected users using any earlier series of Guzzle should upgrade to Guzzle 6.5.8 or 7.4.5. Note that a partial fix was implemented in Guzzle 7.4.2, where a change in host would trigger removal of the curl-added Authorization header, however this earlier fix did not cover change in scheme or change in port. An alternative approach would be to use your own redirect middleware, rather than ours, if you are unable to upgrade. If you do not require or expect redirects to be followed, one should simply disable redirects all together.

**CVSS V2:** AV:N/AC:L/Au:S/C:P/I:N/A:N

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N

**CWE:** NVD-CWE-noinfo

**References:**

- <https://github.com/guzzle/guzzle/commit/1dd98b0564cb3f6bd16ce683cb755f94c10fdbd82>
- <https://github.com/guzzle/guzzle/security/advisories/GHSA-q559-8m2m-g699>
- <https://www.debian.org/security/2022/dsa-5246>

**Package:** guzzlehttp/guzzle

**Version:** 7.4.4

**CVE:** CVE-2022-31090

**Title:** Exposure of Sensitive Information to an Unauthorized Actor

**Description:** Guzzle, an extensible PHP HTTP client. `Authorization` headers on requests are sensitive information. In affected versions when using our Curl handler, it is possible to use the `CURLOPT\_HTTPAUTH` option to specify an `Authorization` header. On making a request which responds with a redirect to a URI with a different origin (change in host, scheme or port), if we choose to follow it, we should remove the `CURLOPT\_HTTPAUTH` option before continuing, stopping curl from appending the `Authorization` header to the new request. Affected Guzzle 7 users should upgrade to Guzzle 7.4.5 as soon as possible. Affected users using any earlier series of Guzzle should upgrade to Guzzle 6.5.8 or 7.4.5. Note that a partial fix was implemented in Guzzle 7.4.2, where a change in host would trigger removal of the curl-added Authorization header, however this earlier fix did not cover change in scheme or change in port. If you do not require or expect redirects to be followed, one should simply disable redirects all together. Alternatively, one can specify to use the Guzzle steam handler backend, rather than curl.

**CVSS V2:** AV:N/AC:L/Au:S/C:P/I:N/A:N

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N

**CWE:** CWE-200

**References:**

- <https://github.com/guzzle/guzzle/commit/1dd98b0564cb3f6bd16ce683cb755f94c10fdbd82>
- <https://github.com/guzzle/guzzle/security/advisories/GHSA-25mq-v84q-4j7r>
- <https://www.debian.org/security/2022/dsa-5246>

**Package:** knplabs/knp-snappy

**Version:** 1.4.1

**CVE:** CVE-2023-28115

**Title:** Deserialization of Untrusted Data

**Description:** Snappy is a PHP library allowing thumbnail, snapshot or PDF generation from a url or a html page. Prior to version 1.4.2, Snappy is vulnerable to PHAR deserialization due to a lack of checking on the protocol before passing it into the `file\_exists()` function. If an attacker can upload files of any type to the server he can pass in the phar:// protocol to unserialize the uploaded file and instantiate arbitrary PHP objects. This can lead to remote code execution especially when snappy is used with frameworks with documented POP chains like Laravel/Symfony vulnerable developer code. If a user can control the output file from the `generateFromHtml()` function, it will invoke deserialization. This vulnerability is capable of remote code execution if Snappy is used with frameworks or developer code with vulnerable POP chains. It has been fixed in version 1.4.2.

**CVSS V2:**

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

**CWE:** CWE-502

**References:**

- <https://github.com/KnpLabs/snappy/releases/tag/v1.4.2>
- <https://github.com/KnpLabs/snappy/security/advisories/GHSA-gq6w-q6wh-jggc>
- <https://github.com/KnpLabs/snappy/commit/b66f79334421c26d9c244427963fa2d92980b5d3>
- <https://github.com/KnpLabs/snappy/commit/1ee6360cbdbea5d09705909a150df7963a88efd6>
- <https://github.com/KnpLabs/snappy/blob/5126fb5b335ec929a226314d40cd8dad497c3d67/src/Knp/Snappy/AbstractGenerator.php#L670>

- <https://github.com/KnpLabs/snappy/pull/469>

**Package:** phpseclib/phpseclib

**Version:** 2.0.37

**CVE:** CVE-2023-27560

**Title:** Loop with Unreachable Exit Condition ('Infinite Loop')

**Description:** Math/PrimeField.php in phpseclib 3.x before 3.0.19 has an infinite loop with composite primefields.

**CVSS V2:**

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

**CWE:** CWE-835

**References:**

- <https://github.com/phpseclib/phpseclib/commit/6298d1cd55c3ffa44533bd41906caec246b60440>
- <https://github.com/phpseclib/phpseclib/releases/tag/3.0.19>

**Package:** smarty/smarty

**Version:** 2.6.33

**CVE:** CVE-2021-26119

**Title:**

**Description:** Smarty before 3.1.39 allows a Sandbox Escape because \$smarty.template\_object can be accessed in

sandbox mode.

**CVSS V2:** AV:N/AC:L/Au:N/C:N/I:P/A:N

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

**CWE:** NVD-CWE-noinfo

**References:**

- <https://github.com/smarty-php/smarty/blob/master/CHANGELOG.md>
- <https://lists.debian.org/debian-lts-announce/2021/04/msg00004.html>
- <https://lists.debian.org/debian-lts-announce/2021/04/msg00014.html>
- <https://security.gentoo.org/glsa/202105-06>
- <https://www.debian.org/security/2022/dsa-5151>

**Package:** smarty/smarty

**Version:** 2.6.33

**CVE:** CVE-2021-26120

**Title:** Improper Control of Generation of Code ('Code Injection')

**Description:** Smarty before 3.1.39 allows code injection via an unexpected function name after a {function name= substring.

**CVSS V2:** AV:N/AC:L/Au:N/C:P/I:P/A:P

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

**CWE:** CWE-94

**References:**

- <https://github.com/smarty-php/smarty/blob/master/CHANGELOG.md>
- <https://lists.debian.org/debian-lts-announce/2021/04/msg00004.html>
- <https://lists.debian.org/debian-lts-announce/2021/04/msg00014.html>
- <https://security.gentoo.org/glsa/202105-06>
- <https://www.debian.org/security/2022/dsa-5151>

**Package:** smarty/smarty

**Version:** 2.6.33

**CVE:** CVE-2017-1000480

**Title:** Improper Control of Generation of Code ('Code Injection')

**Description:** Smarty 3 before 3.1.32 is vulnerable to a PHP code injection when calling fetch() or display() functions on custom resources that does not sanitize template name.

**CVSS V2:** AV:N/AC:L/Au:N/C:P/I:P/A:P

**CVSS V3:** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

**CWE:** CWE-94

**References:**

- [https://github.com/smarty-php/smarty/blob/master/change\\_log.txt](https://github.com/smarty-php/smarty/blob/master/change_log.txt)
- <https://www.debian.org/security/2018/dsa-4094>
- <https://lists.debian.org/debian-lts-announce/2018/02/msg00000.html>
- <https://lists.debian.org/debian-lts-announce/2018/01/msg00023.html>

**Package:** smarty/smarty

**Version:** 2.6.33

**CVE:** CVE-2018-13982

**Title:** Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

**Description:** Smarty\_Security::isTrustedResourceDir() in Smarty before 3.1.33 is prone to a path traversal vulnerability due to insufficient template code sanitization. This allows attackers controlling the executed template code to bypass the trusted directory security restriction and read arbitrary files.

**CVSS V2:** AV:N/AC:L/Au:N/C:P/I:N/A:N

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

**CWE:** CWE-22

**References:**

- <https://github.com/smarty-php/smarty/commit/f9ca3c63d1250bb56b2bda609dcc9dd81f0065f8>
- <https://github.com/smarty-php/smarty/commit/c9dbe1d08c081912d02bd851d1d1b6388f6133d1>
- <https://github.com/smarty-php/smarty/commit/bcedfd6b58bed4a7366336979ebaa5a240581531>
- <https://github.com/smarty-php/smarty/commit/8d21f38dc35c4cd6b31c2f23fc9b8e5adbc56dfe>
- <https://github.com/smarty-php/smarty/commit/2e081a51b1effdb23f87952959139ac62654d50>
- [https://github.com/sbaresearch/advisories/tree/public/2018/SBA-ADV-20180420-01\\_Smarty\\_Path\\_Traversal](https://github.com/sbaresearch/advisories/tree/public/2018/SBA-ADV-20180420-01_Smarty_Path_Traversal)
- <https://lists.debian.org/debian-lts-announce/2021/04/msg00004.html>
- <https://lists.debian.org/debian-lts-announce/2021/04/msg00014.html>
- <https://lists.debian.org/debian-lts-announce/2021/10/msg00015.html>

**Package:** smarty/smarty

**Version:** 2.6.33

**CVE:** CVE-2021-21408

**Title:** Improper Input Validation

**Description:** Smarty is a template engine for PHP, facilitating the separation of presentation (HTML/CSS) from application logic. Prior to versions 3.1.43 and 4.0.3, template authors could run restricted static php methods. Users should upgrade to version 3.1.43 or 4.0.3 to receive a patch.

**CVSS V2:** AV:N/AC:L/Au:S/C:P/I:P/A:P

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

**CWE:** CWE-20

**References:**

- <https://github.com/smarty-php/smarty/commit/19ae410bf56007a5ef24441cdc6414619cfaf664>
- <https://github.com/smarty-php/smarty/releases/tag/v3.1.43>
- <https://github.com/smarty-php/smarty/security/advisories/GHSA-4h9c-v5vg-5m6m>
- <https://github.com/smarty-php/smarty/releases/tag/v4.0.3>
- <https://lists.debian.org/debian-lts-announce/2022/05/msg00005.html>
- <https://www.debian.org/security/2022/dsa-5151>
- <https://security.gentoo.org/glsa/202209-09>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/L777JIBIWJV34HS7LXPIDWASG7TT4LNI/>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/BRAJVDRGCIY5UZ2PQHKDTT7RMKG6WJQQ/>

**Package:** smarty/smarty

**Version:** 2.6.33

**CVE:** CVE-2021-29454

**Title:** Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')

**Description:** Smarty is a template engine for PHP, facilitating the separation of presentation (HTML/CSS) from application logic. Prior to versions 3.1.42 and 4.0.2, template authors could run arbitrary PHP code by crafting a malicious math string. If a math string was passed through as user provided data to the math function, external users could run arbitrary PHP code by crafting a malicious math string. Users should upgrade to version 3.1.42 or 4.0.2 to receive a patch.

**CVSS V2:** AV:N/AC:L/Au:S/C:P/I:P/A:P

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

**CWE:** CWE-74

**References:**

- <https://github.com/smarty-php/smarty/commit/215d81a9fa3cd63d82fb3ab56ecaf97cf1e7db71>
- <https://github.com/smarty-php/smarty/security/advisories/GHSA-29gp-2c3m-3j6m>
- <https://packagist.org/packages/smarty/smarty>
- <https://github.com/smarty-php/smarty/releases/tag/v3.1.42>
- <https://www.smarty.net/docs/en/language.function.math.tpl>
- <https://github.com/smarty-php/smarty/releases/tag/v4.0.2>
- <https://lists.debian.org/debian-lts-announce/2022/05/msg00005.html>
- <https://www.debian.org/security/2022/dsa-5151>
- <https://security.gentoo.org/glsa/202209-09>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/L777JIBIWJV34HS7LXPIDWASG7TT4LNI/>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/BRAJVDRGCIY5UZ2PQHKDTT7RMKG6WJQQ/>

**Package:** smarty/smarty

**Version:** 2.6.33

**CVE:** CVE-2022-29221

**Title:** Improper Control of Generation of Code ('Code Injection')

**Description:** Smarty is a template engine for PHP, facilitating the separation of presentation (HTML/CSS) from application logic. Prior to versions 3.1.45 and 4.1.1, template authors could inject php code by choosing a malicious {block} name or {include} file name. Sites that cannot fully trust template authors should upgrade to versions 3.1.45 or 4.1.1 to receive a patch for this issue. There are currently no known workarounds.

**CVSS V2:** AV:N/AC:L/Au:S/C:P/I:P/A:P

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

**CWE:** CWE-94

**References:**

- <https://github.com/smarty-php/smarty/releases/tag/v3.1.45>
- <https://github.com/smarty-php/smarty/security/advisories/GHSA-634x-pc3q-cf4c>
- <https://github.com/smarty-php/smarty/commit/64ad6442ca1da31cefdb5c9874262b702ccddd>
- <https://github.com/smarty-php/smarty/releases/tag/v4.1.1>
- <https://www.debian.org/security/2022/dsa-5151>
- <https://lists.debian.org/debian-lts-announce/2022/05/msg00044.html>
- <https://security.gentoo.org/glsa/202209-09>

- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/L777JIBIWJV34HS7LXPIDWASG7TT4LNI/>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/BRAJVDRGCIY5UZ2PQHKDTT7RMKG6WJQQ/>

**Package:** twig/twig

**Version:** 3.4.1

**CVE:** CVE-2022-39261

**Title:** Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

**Description:** Twig is a template language for PHP. Versions 1.x prior to 1.44.7, 2.x prior to 2.15.3, and 3.x prior to 3.4.3 encounter an issue when the filesystem loader loads templates for which the name is a user input. It is possible to use the `source` or `include` statement to read arbitrary files from outside the templates' directory when using a namespace like `@somewhere/..//some.file`. In such a case, validation is bypassed. Versions 1.44.7, 2.15.3, and 3.4.3 contain a fix for validation of such template names. There are no known workarounds aside from upgrading.

**CVSS V2:**

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

**CWE:** CWE-22

**References:**

- <https://github.com/twigphp/Twig/commit/35f3035c5deb0041da7b84daf02dea074ddc7a0b>
- <https://github.com/twigphp/Twig/security/advisories/GHSA-52m2-vc4m-jj33>
- <https://www.drupal.org/sa-core-2022-016>
- <https://www.debian.org/security/2022/dsa-5248>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/2OKRUHPVLIQVFPPJ2UWC3WV3WQO763NR/>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/AUVTXMNPSZAHS3DWZEM56V5W4NPVR6L7/>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/NWRFPZSR74SYVJKBTKTMYUK36IJ3SQJP/>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/YU4ZYX62H2NUAKKGUES4RZIM4KMTKZ7F/>
- <https://lists.debian.org/debian-lts-announce/2022/10/msg00016.html>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/TW53TFJ6WWNXMUHOFACKATJTS7NIHVQE/>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/WV5TNNJLGG536TJH6DLCIAAZZIPV2GUD/>

## <http://192.168.145.128/openemr/>

List of vulnerable **composer** packages:

**Package:** dompdf/dompdf

**Version:** 1.2.2

**CVE:** CVE-2022-41343

**Title:** Files or Directories Accessible to External Parties

**Description:** registerFont in FontMetrics.php in Dompdf before 2.0.1 allows remote file inclusion because a URI validation failure does not halt font registration, as demonstrated by a @font-face rule.

**CVSS V2:**

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

**CWE:** CWE-552

**References:**

- <https://github.com/dompdf/dompdf/releases/tag/v2.0.1>
- <https://github.com/dompdf/dompdf/issues/2994>
- <https://github.com/dompdf/dompdf/pull/2995>
- <https://tantosec.com/blog/cve-2022-41343/>

**Package:** dompdf/dompdf

**Version:** 1.2.2

**CVE:** CVE-2023-23924

**Title:** Incorrect Authorization

**Description:** Dompdf is an HTML to PDF converter. The URI validation on dompdf 2.0.1 can be bypassed on SVG parsing by passing `<image>` tags with uppercase letters. This may lead to arbitrary object unserialize on PHP < 8, through the `phar` URL wrapper. An attacker can exploit the vulnerability to call arbitrary URL with arbitrary protocols, if they can provide a SVG file to dompdf. In PHP versions before 8.0.0, it leads to arbitrary unserialize, that will lead to the very least to an arbitrary file deletion and even remote code execution, depending on classes that are available.

**CVSS V2:**

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

**CWE:** CWE-863

**References:**

- <https://github.com/dompdf/dompdf/security/advisories/GHSA-3cw5-7cxw-v5qg>
- <https://github.com/dompdf/dompdf/releases/tag/v2.0.2>
- <https://github.com/dompdf/dompdf/commit/7558f07f693b2ac3266089f21051e6b78c6a0c85>

**Package:** dompdf/dompdf

**Version:** 1.2.2

**CVE:** CVE-2023-24813

**Title:** Interpretation Conflict

**Description:** Dompdf is an HTML to PDF converter written in php. Due to the difference in the attribute parser of Dompdf and php-svg-lib, an attacker can still call arbitrary URLs with arbitrary protocols. Dompdf parses the href attribute of `image` tags and respects `xlink:href` even if `href` is specified. However, php-svg-lib, which is later used to parse the svg file, parses the href attribute. Since `href` is respected if both `xlink:href` and `href` is specified, it's possible to bypass the protection on the Dompdf side by providing an empty `xlink:href` attribute. An attacker can exploit the vulnerability to call arbitrary URLs with arbitrary protocols if they provide an SVG file to the Dompdf. In PHP versions before 8.0.0, it leads to arbitrary unserialize, which will lead, at the very least, to arbitrary file deletion and might lead to remote code execution, depending on available classes. This vulnerability has been addressed in commit `95009ea98` which has been included in release version 2.0.3. Users are advised to upgrade. There are no known workarounds for this vulnerability.

**CVSS V2:**

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

**CWE:** CWE-436

**References:**

- <https://github.com/dompdf/dompdf/security/advisories/GHSA-56gj-mvh6-rp75>
- <https://github.com/dompdf/dompdf/commit/95009ea98230f9b084b040c34e3869ef3dccc9aa>

**Package:** guzzlehttp/guzzle

**Version:** 7.4.4

**CVE:** CVE-2022-31091

**Title:**

**Description:** Guzzle, an extensible PHP HTTP client. `Authorization` and `Cookie` headers on requests are sensitive information. In affected versions on making a request which responds with a redirect to a URI with a different port, if we choose to follow it, we should remove the `Authorization` and `Cookie` headers from the request, before containing. Previously, we would only consider a change in host or scheme. Affected Guzzle 7 users should upgrade to Guzzle 7.4.5 as soon as possible. Affected users using any earlier series of Guzzle should upgrade to Guzzle 6.5.8 or 7.4.5. Note that a partial fix was implemented in Guzzle 7.4.2, where a change in host would trigger removal of the curl-added Authorization header, however this earlier fix did not cover change in scheme or change in port. An alternative approach would be to use your own redirect middleware, rather than ours, if you are unable to upgrade. If you do not require or expect redirects to be followed, one should simply disable redirects all together.

**CVSS V2:** AV:N/AC:L/Au:S/C:P/I:N/A:N

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

**CWE:** NVD-CWE-noinfo

**References:**

- <https://github.com/guzzle/guzzle/commit/1dd98b0564cb3f6bd16ce683cb755f94c10fdbd82>
- <https://github.com/guzzle/guzzle/security/advisories/GHSA-q559-8m2m-g699>
- <https://www.debian.org/security/2022/dsa-5246>

**Package:** guzzlehttp/guzzle

**Version:** 7.4.4

**CVE:** CVE-2022-31090

**Title:** Exposure of Sensitive Information to an Unauthorized Actor

**Description:** Guzzle, an extensible PHP HTTP client. `Authorization` headers on requests are sensitive information. In affected versions when using our Curl handler, it is possible to use the `CURLOPT\_HTTPAUTH` option to specify an `Authorization` header. On making a request which responds with a redirect to a URI with a different origin (change in host, scheme or port), if we choose to follow it, we should remove the `CURLOPT\_HTTPAUTH` option before continuing, stopping curl from appending the `Authorization` header to the new request. Affected Guzzle 7 users should upgrade to Guzzle 7.4.5 as soon as possible. Affected users using any earlier series of Guzzle should upgrade to Guzzle 6.5.8 or 7.4.5. Note that a partial fix was implemented in Guzzle 7.4.2, where a change in host would trigger removal of the curl-added Authorization header, however this earlier fix did not cover change in scheme or change in port. If you do not require or expect redirects to be followed, one should simply disable redirects all together. Alternatively, one can specify to use the Guzzle steam handler backend, rather than curl.

**CVSS V2:** AV:N/AC:L/Au:S/C:P/I:N/A:N

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

**CWE:** CWE-200

**References:**

- <https://github.com/guzzle/guzzle/commit/1dd98b0564cb3f6bd16ce683cb755f94c10fdb82>
- <https://github.com/guzzle/guzzle/security/advisories/GHSA-25mq-v84q-4j7r>
- <https://www.debian.org/security/2022/dsa-5246>

**Package:** knplabs/knp-snappy

**Version:** 1.4.1

**CVE:** CVE-2023-28115

**Title:** Deserialization of Untrusted Data

**Description:** Snappy is a PHP library allowing thumbnail, snapshot or PDF generation from a url or a html page. Prior to version 1.4.2, Snappy is vulnerable to PHAR deserialization due to a lack of checking on the protocol before passing it into the `file\_exists()` function. If an attacker can upload files of any type to the server he can pass in the phar:// protocol to unserialize the uploaded file and instantiate arbitrary PHP objects. This can lead to remote code execution especially when snappy is used with frameworks with documented POP chains like Laravel/Symfony vulnerable developer code. If a user can control the output file from the `generateFromHtml()` function, it will invoke deserialization. This vulnerability is capable of remote code execution if Snappy is used with frameworks or developer code with vulnerable POP chains. It has been fixed in version 1.4.2.

**CVSS V2:**

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

**CWE:** CWE-502

**References:**

- <https://github.com/KnpLabs/snappy/releases/tag/v1.4.2>
- <https://github.com/KnpLabs/snappy/security/advisories/GHSA-gq6w-q6wh-jggc>
- <https://github.com/KnpLabs/snappy/commit/b66f79334421c26d9c244427963fa2d92980b5d3>
- <https://github.com/KnpLabs/snappy/commit/1ee6360cbdbea5d09705909a150df7963a88efd6>
- <https://github.com/KnpLabs/snappy/blob/5126fb5b335ec929a226314d40cd8dad497c3d67/src/Knp/Snappy/AbstractGenerator.php#L670>

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

**Package:** phpseclib/phpseclib

**Version:** 2.0.37

**CVE:** CVE-2023-27560

**Title:** Loop with Unreachable Exit Condition ('Infinite Loop')

**Description:** Math/PrimeField.php in phpseclib 3.x before 3.0.19 has an infinite loop with composite primefields.

**CVSS V2:**

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

**CWE:** CWE-835

**References:**

- <https://github.com/phpseclib/phpseclib/commit/6298d1cd55c3ffa44533bd41906caec246b60440>
- <https://github.com/phpseclib/phpseclib/releases/tag/3.0.19>

**Package:** smarty/smarty

**Version:** 2.6.33

**CVE:** CVE-2021-26119

**Title:**

**Description:** Smarty before 3.1.39 allows a Sandbox Escape because \$smarty.template\_object can be accessed in sandbox mode.

**CVSS V2:** AV:N/AC:L/Au:N/C:N/I:P/A:N

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

**CWE:** NVD-CWE-noinfo

**References:**

- <https://github.com/smarty-php/smarty/blob/master/CHANGELOG.md>
- <https://lists.debian.org/debian-lts-announce/2021/04/msg00004.html>
- <https://lists.debian.org/debian-lts-announce/2021/04/msg00014.html>
- <https://security.gentoo.org/glsa/202105-06>
- <https://www.debian.org/security/2022/dsa-5151>

**Package:** smarty/smarty

**Version:** 2.6.33

**CVE:** CVE-2021-26120

**Title:** Improper Control of Generation of Code ('Code Injection')

**Description:** Smarty before 3.1.39 allows code injection via an unexpected function name after a {function name= substring.

**CVSS V2:** AV:N/AC:L/Au:N/C:P/I:P/A:P

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

**CWE:** CWE-94

**References:**

- <https://github.com/smarty-php/smarty/blob/master/CHANGELOG.md>
- <https://lists.debian.org/debian-lts-announce/2021/04/msg00004.html>
- <https://lists.debian.org/debian-lts-announce/2021/04/msg00014.html>
- <https://security.gentoo.org/glsa/202105-06>
- <https://www.debian.org/security/2022/dsa-5151>

**Package:** smarty/smarty

**Version:** 2.6.33

**CVE:** CVE-2017-1000480

**Title:** Improper Control of Generation of Code ('Code Injection')

**Description:** Smarty 3 before 3.1.32 is vulnerable to a PHP code injection when calling fetch() or display() functions on custom resources that does not sanitize template name.

**CVSS V2:** AV:N/AC:L/Au:N/C:P/I:P/A:P

**CVSS V3:** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

**CWE:** CWE-94

**References:**

- [https://github.com/smarty-php/smarty/blob/master/change\\_log.txt](https://github.com/smarty-php/smarty/blob/master/change_log.txt)
- <https://www.debian.org/security/2018/dsa-4094>

- <https://lists.debian.org/debian-lts-announce/2018/02/msg00000.html>
- <https://lists.debian.org/debian-lts-announce/2018/01/msg00023.html>

**Package:** smarty/smarty

**Version:** 2.6.33

**CVE:** CVE-2018-13982

**Title:** Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

**Description:** Smarty\_Security::isTrustedResourceDir() in Smarty before 3.1.33 is prone to a path traversal vulnerability due to insufficient template code sanitization. This allows attackers controlling the executed template code to bypass the trusted directory security restriction and read arbitrary files.

**CVSS V2:** AV:N/AC:L/Au:N/C:P/I:N/A:N

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

**CWE:** CWE-22

**References:**

- <https://github.com/smarty-php/smarty/commit/f9ca3c63d1250bb56b2bda609dcc9dd81f0065f8>
- <https://github.com/smarty-php/smarty/commit/c9dbe1d08c081912d02bd851d1d1b6388f6133d1>
- <https://github.com/smarty-php/smarty/commit/bcedfd6b58bed4a7366336979ebaa5a240581531>
- <https://github.com/smarty-php/smarty/commit/8d21f38dc35c4cd6b31c2f23fc9b8e5adbc56dfe>
- <https://github.com/smarty-php/smarty/commit/2e081a51b1effddb23f87952959139ac62654d50>
- [https://github.com/sbaresearch/advisories/tree/public/2018/SBA-ADV-20180420-01\\_Smarty\\_Path\\_Traversal](https://github.com/sbaresearch/advisories/tree/public/2018/SBA-ADV-20180420-01_Smarty_Path_Traversal)
- <https://lists.debian.org/debian-lts-announce/2021/04/msg00004.html>
- <https://lists.debian.org/debian-lts-announce/2021/04/msg00014.html>
- <https://lists.debian.org/debian-lts-announce/2021/10/msg00015.html>

**Package:** smarty/smarty

**Version:** 2.6.33

**CVE:** CVE-2021-21408

**Title:** Improper Input Validation

**Description:** Smarty is a template engine for PHP, facilitating the separation of presentation (HTML/CSS) from application logic. Prior to versions 3.1.43 and 4.0.3, template authors could run restricted static php methods. Users should upgrade to version 3.1.43 or 4.0.3 to receive a patch.

**CVSS V2:** AV:N/AC:L/Au:S/C:P/I:P/A:P

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

**CWE:** CWE-20

**References:**

- <https://github.com/smarty-php/smarty/commit/19ae410bf56007a5ef24441cdc6414619cfaf664>
- <https://github.com/smarty-php/smarty/releases/tag/v3.1.43>
- <https://github.com/smarty-php/smarty/security/advisories/GHSA-4h9c-v5vg-5m6m>
- <https://github.com/smarty-php/smarty/releases/tag/v4.0.3>
- <https://lists.debian.org/debian-lts-announce/2022/05/msg00005.html>
- <https://www.debian.org/security/2022/dsa-5151>
- <https://security.gentoo.org/glsa/202209-09>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/L777JIBIWJV34HS7LXPIDWASG7TT4LNI/>

- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/BRAJVDRGCIY5UZ2PQHKDTT7RMKG6WJQQ/>

**Package:** smarty/smarty

**Version:** 2.6.33

**CVE:** CVE-2021-29454

**Title:** Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')

**Description:** Smarty is a template engine for PHP, facilitating the separation of presentation (HTML/CSS) from application logic. Prior to versions 3.1.42 and 4.0.2, template authors could run arbitrary PHP code by crafting a malicious math string. If a math string was passed through as user provided data to the math function, external users could run arbitrary PHP code by crafting a malicious math string. Users should upgrade to version 3.1.42 or 4.0.2 to receive a patch.

**CVSS V2:** AV:N/AC:L/Au:S/C:P/I:P/A:P

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

**CWE:** CWE-74

**References:**

- <https://github.com/smarty-php/smarty/commit/215d81a9fa3cd63d82fb3ab56ecaf97cf1e7db71>
- <https://github.com/smarty-php/smarty/security/advisories/GHSA-29gp-2c3m-3j6m>
- <https://packagist.org/packages/smarty/smarty>
- <https://github.com/smarty-php/smarty/releases/tag/v3.1.42>
- <https://www.smarty.net/docs/en/language.function.math.tpl>
- <https://github.com/smarty-php/smarty/releases/tag/v4.0.2>
- <https://lists.debian.org/debian-lts-announce/2022/05/msg00005.html>
- <https://www.debian.org/security/2022/dsa-5151>
- <https://security.gentoo.org/glsa/202209-09>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/L777JIBIWJV34HS7LXPIDWASG7TT4LNI/>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/BRAJVDRGCIY5UZ2PQHKDTT7RMKG6WJQQ/>

**Package:** smarty/smarty

**Version:** 2.6.33

**CVE:** CVE-2022-29221

**Title:** Improper Control of Generation of Code ('Code Injection')

**Description:** Smarty is a template engine for PHP, facilitating the separation of presentation (HTML/CSS) from application logic. Prior to versions 3.1.45 and 4.1.1, template authors could inject php code by choosing a malicious {block} name or {include} file name. Sites that cannot fully trust template authors should upgrade to versions 3.1.45 or 4.1.1 to receive a patch for this issue. There are currently no known workarounds.

**CVSS V2:** AV:N/AC:L/Au:S/C:P/I:P/A:P

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

**CWE:** CWE-94

**References:**

- <https://github.com/smarty-php/smarty/releases/tag/v3.1.45>
- <https://github.com/smarty-php/smarty/security/advisories/GHSA-634x-pc3q-cf4c>
- <https://github.com/smarty-php/smarty/commit/64ad6442ca1da31cefdab5c9874262b702ccddd>

- <https://github.com/smarty-php/smarty/releases/tag/v4.1.1>
- <https://www.debian.org/security/2022/dsa-5151>
- <https://lists.debian.org/debian-lts-announce/2022/05/msg00044.html>
- <https://security.gentoo.org/glsa/202209-09>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/L777JIBIWJV34HS7LXPIDWASG7TT4LNI/>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/BRAJVDRGCIY5UZ2PQHKDTT7RMKG6WJQQ/>

**Package:** twig/twig

**Version:** 3.4.1

**CVE:** CVE-2022-39261

**Title:** Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

**Description:** Twig is a template language for PHP. Versions 1.x prior to 1.44.7, 2.x prior to 2.15.3, and 3.x prior to 3.4.3 encounter an issue when the filesystem loader loads templates for which the name is a user input. It is possible to use the `source` or `include` statement to read arbitrary files from outside the templates' directory when using a namespace like `@somewhere/..//some.file`. In such a case, validation is bypassed. Versions 1.44.7, 2.15.3, and 3.4.3 contain a fix for validation of such template names. There are no known workarounds aside from upgrading.

**CVSS V2:**

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

**CWE:** CWE-22

**References:**

- <https://github.com/twigphp/Twig/commit/35f3035c5deb0041da7b84daf02dea074ddc7a0b>
- <https://github.com/twigphp/Twig/security/advisories/GHSA-52m2-vc4m-jj33>
- <https://www.drupal.org/sa-core-2022-016>
- <https://www.debian.org/security/2022/dsa-5248>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/2OKRUHPVLIQVFPPJ2UWC3WV3WQO763NR/>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/AUVTXMNPSZAHS3DWZEM56V5W4NPVR6L7/>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/NWRFPZSR74SYVJKBTKTMYUK36IJ3SQJP/>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/YU4ZYX62H2NUAKKGUES4RZIM4KMTKZ7F/>
- <https://lists.debian.org/debian-lts-announce/2022/10/msg00016.html>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/TW53TFJ6WWNXMUHOFACKATJTS7NIHVQE/>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/WV5TNNJLGG536TJH6DLCIAAZZIPV2GUD/>

## Recommendation

---

It's recommended to update the vulnerable packages to the latest version (if a fix exists). If a fix does not exist, you may want to suggest changes that address the vulnerability to the package maintainer or remove the package from your dependency tree.

## Vulnerable JavaScript libraries

---

You are using one or more vulnerable JavaScript libraries. One or more vulnerabilities were reported for this version of the library. Consult Attack details and Web References for more information about the affected library and the vulnerabilities that were reported.

### CWE

CWE-937

### CVSS2

AV:N/AC:L/Au:N/C:P/I:P/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	Partial
Availability Impact	None

### CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N

Base Score	6.5
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	Low
Availability Impact	None

## Impact

---

Consult References for more information.

<http://10.10.236.31/>

Confidence: 95%

- **jQuery 1.10.2**
  - URL: <http://10.10.236.31/openemr/public/assets/jquery-datetimepicker/>
  - Detection method: The library's name and version were determined based on its dynamic behavior.
  - CVE-ID: CVE-2015-9251, CVE-2020-11022, CVE-2020-11023
  - Description: Possible Cross Site Scripting via third-party text/javascript responses / In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. / In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing option elements from untrusted sources - even after sanitizing it - to one of

jQuery's DOM manipulation methods (i.e. `.html()`, `.append()`, and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

- o References:

- <https://github.com/jquery/jquery/issues/2432>
- <http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/>
- <https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/>
- <https://mksben.l0.cm/2020/05/jquery3.5.0-xss.html>
- <https://jquery.com/upgrade-guide/3.5/>
- <https://api.jquery.com/jQuery.htmlPrefilter/>
- <https://www.cvedetails.com/cve/CVE-2020-11022/>
- <https://github.com/advisories/GHSA-gxr4-xjj5-px2>
- <https://www.cvedetails.com/cve/CVE-2020-11023/>
- <https://github.com/advisories/GHSA-jpcq-cgw6-v4j6>

## Request

```
GET /openemr/public/assets/jquery-datetimepicker/ HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 8595e182db21cbbc10c83c2c4cf193d3
Acunetix-Aspect-ScanID: 816589585389164376
Acunetix-Aspect-Queries: filelist;packages;aspectalerts;routes
Referer: http://10.10.236.31/openemr/public/assets/jquery-datetimepicker/
Cookie: OpenEMR=Dj68HNoGw-vYWT2k81NHDiqIHhLtRgfoVY0Tqo%2Cj6JeJm5aU
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 10.10.236.31
Connection: Keep-alive
```

## <http://10.10.236.31/>

Verified

- **jQuery UI 1.12.1**

- o URL: <http://10.10.236.31/openemr/public/assets/jquery-ui/jquery-ui.js>
- o Detection method: The library's name and version were determined based on the file's syntax fingerprint, and contents. Acunetix verified the library version and the associated vulnerabilities with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- o CVE-ID: CVE-2021-41184
- o Description: XSS in the 'of' option of the '.position()' util
- o References:
  - <https://blog.jqueryui.com/2021/10/jquery-ui-1-13-0-released/>
  - <https://github.com/jquery/jquery-ui/security/advisories/GHSA-gpqq-952q-5327>

## Request

```
GET /openemr/public/assets/jquery-ui/jquery-ui.js HTTP/1.1
Acunetix-Aspect: enabled
```

Acunetix-Aspect-Password: 8595e182db21cbbc10c83c2c4cf193d3  
Acunetix-Aspect-ScanID: 816589585389164376  
Acunetix-Aspect-Queries: aspectalerts;routes  
Referer: http://10.10.236.31/openemr/Documentation/help\_files/openemr\_installation\_help.php  
Cookie: OpenEMR=b3DHM9s5BR72IjC3y6GcpBb736abtMj3%2CfzaSNeoS-j94pMx  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
Accept-Encoding: gzip,deflate,br  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)  
Chrome/109.0.0.0 Safari/537.36  
Host: 10.10.236.31  
Connection: Keep-alive

**http://10.10.236.31/**

Confidence: 95%

- **jQuery UI Datepicker 1.12.1**

- URL: <http://10.10.236.31/openemr/public/assets/jquery-ui/jquery-ui.js>
- Detection method: The library's name and version were determined based on the file's contents.
- CVE-ID: CVE-2021-41182, CVE-2021-41183
- Description: XSS in the 'altField' option of the Datepicker widget / XSS in '\*Text' options of the Datepicker widget
- References:
  - <https://blog.jqueryui.com/2021/10/jquery-ui-1-13-0-released/>
  - <https://github.com/jquery/jquery-ui/security/advisories/GHSA-9gj3-hwp5-pmwc>
  - <https://github.com/jquery/jquery-ui/security/advisories/GHSA-j7qv-pgf6-hvh4>

## Request

GET /openemr/public/assets/jquery-ui/jquery-ui.js HTTP/1.1  
Acunetix-Aspect: enabled  
Acunetix-Aspect-Password: 8595e182db21cbbc10c83c2c4cf193d3  
Acunetix-Aspect-ScanID: 816589585389164376  
Acunetix-Aspect-Queries: aspectalerts;routes  
Referer: http://10.10.236.31/openemr/Documentation/help\_files/openemr\_installation\_help.php  
Cookie: OpenEMR=b3DHM9s5BR72IjC3y6GcpBb736abtMj3%2CfzaSNeoS-j94pMx  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
Accept-Encoding: gzip,deflate,br  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)  
Chrome/109.0.0.0 Safari/537.36  
Host: 10.10.236.31  
Connection: Keep-alive

**http://10.10.236.31/**

Verified

- **jQuery 1.12.4**

- URL: <http://10.10.236.31/openemr/public/assets/jquery-ui/external/jquery/jquery.js>

- Detection method: The library's name and version were determined based on the file's syntax fingerprint, and contents. Acunetix verified the library version and the associated vulnerabilities with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- CVE-ID: CVE-2015-9251, CVE-2020-11022, CVE-2020-11023
- Description: Possible Cross Site Scripting via third-party text/javascript responses (1.12.0-1.12.2 mitigation reverted) / In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. / In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing option elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.
- References:
  - <https://github.com/jquery/jquery/issues/2432>
  - <https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/>
  - <https://mksben.l0.cm/2020/05/jquery3.5.0-xss.html>
  - <https://jquery.com/upgrade-guide/3.5/>
  - <https://api.jquery.com/jQuery.htmlPrefilter/>
  - <https://www.cvedetails.com/cve/CVE-2020-11022/>
  - <https://github.com/advisories/GHSA-gxr4-xjj5-5px2>
  - <https://www.cvedetails.com/cve/CVE-2020-11023/>
  - <https://github.com/advisories/GHSA-jpcq-cgw6-v4j6>

## Request

---

```
GET /openemr/public/assets/jquery-ui/external/jquery/jquery.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 8595e182db21cbbc10c83c2c4cf193d3
Acunetix-Aspect-ScanID: 816589585389164376
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://10.10.236.31/openemr/public/assets/jquery-ui/
Cookie: OpenEMR=b3DHM9s5BR72IjC3y6GcpBb736abtMj3%2CfzaSNeoS-j94pMx
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 10.10.236.31
Connection: Keep-alive
```

<http://192.168.145.128/>

Confidence: 95%

- AngularJS 1.4.8
  - URL: <https://cdnjs.cloudflare.com/ajax/libs/angular.js/1.4.8/angular.js>
  - Detection method: The library's name and version were determined based on the file's CDN URI.
  - CVE-ID: CVE-2020-7676
  - Description: Prototype pollution / Cross-Site Scripting.
  - References:

- <https://github.com/angular/angular.js/commit/726f49dcf6c23106ddaf5cf5e2e592841db743a>
- <https://github.com/angular/angular.js/blob/master/CHANGELOG.md#179-pollution-eradication-2019-11-19>
- <https://nvd.nist.gov/vuln/detail/CVE-2020-7676>

## Request

---

```
GET /openemr/public/assets/checklist-model/ HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/public/assets/
Cookie: OpenEMR=g3GhfkD5xIsb3Ge5m8KYxfe43LFtvIbo%2CVxmCKL9iQGY052L
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

<http://192.168.145.128/>

Verified

- **jQuery UI 1.12.1**

- URL: <http://192.168.145.128/openemr/public/assets/jquery-ui/jquery-ui.js>
- Detection method: The library's name and version were determined based on the file's syntax fingerprint, and contents. Acunetix verified the library version and the associated vulnerabilities with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- CVE-ID: [CVE-2021-41184](#)
- Description: XSS in the 'of' option of the '.position()' util
- References:
  - <https://blog.jqueryui.com/2021/10/jquery-ui-1-13-0-released/>
  - <https://github.com/jquery/jquery-ui/security/advisories/GHSA-gpqq-952q-5327>

## Request

---

```
GET /openemr/public/assets/jquery-ui/jquery-ui.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/Documentation/help_files/openemr_installation_help.php
Cookie: OpenEMR=d40D5DeYlSqGsuSImcMvd1XbnUvSB1S1%2CNItqLcdHnpIKp4G
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
```

<http://192.168.145.128/>

Confidence: 95%

- jQuery UI Datepicker 1.12.1

- URL: <http://192.168.145.128/openemr/public/assets/jquery-ui/jquery-ui.js>
- Detection method: The library's name and version were determined based on the file's contents.
- CVE-ID: CVE-2021-41182, CVE-2021-41183
- Description: XSS in the 'altField' option of the Datepicker widget / XSS in '\*Text' options of the Datepicker widget
- References:
  - <https://blog.jqueryui.com/2021/10/jquery-ui-1-13-0-released/>
  - <https://github.com/jquery/jquery-ui/security/advisories/GHSA-9gj3-hwp5-pmw>
  - <https://github.com/jquery/jquery-ui/security/advisories/GHSA-j7qv-pgf6-hvh4>

## Request

---

```
GET /openemr/public/assets/jquery-ui/jquery-ui.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58adee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/Documentation/help_files/openemr_installation_help.php
Cookie: OpenEMR=d4D5DeYlSqGsuSImcMvd1XbnUvSB1S1%2CNItgLcdHnpIKp4G
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

<http://192.168.145.128/>

Verified

- jQuery 1.12.4

- URL: <http://192.168.145.128/openemr/public/assets/jquery-ui/external/jquery/jquery.js>
- Detection method: The library's name and version were determined based on the file's syntax fingerprint, and contents. Acunetix verified the library version and the associated vulnerabilities with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- CVE-ID: CVE-2015-9251, CVE-2020-11022, CVE-2020-11023
- Description: Possible Cross Site Scripting via third-party text/javascript responses (1.12.0-1.12.2 mitigation reverted) / In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. / In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing option elements from untrusted sources -

even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

- o References:

- <https://github.com/jquery/jquery/issues/2432>
- <https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/>
- <https://mksben.lo.cm/2020/05/jquery3.5.0-xss.html>
- <https://jquery.com/upgrade-guide/3.5/>
- <https://api.jquery.com/jQuery.htmlPrefilter/>
- <https://www.cvedetails.com/cve/CVE-2020-11022/>
- <https://github.com/advisories/GHSA-gxr4-xjj5-5px2>
- <https://www.cvedetails.com/cve/CVE-2020-11023/>
- <https://github.com/advisories/GHSA-jpcq-cgw6-v4j6>

## Request

---

```
GET /openemr/public/assets/jquery-ui/external/jquery/jquery.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/public/assets/jquery-ui/
Cookie: OpenEMR=6WeVd6ZCNQZ1gcdzS-0v%2CJShmKVZumFVDGJv2At8hAWUVEJ3
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

## <http://192.168.145.128/>

Verified

- **jQuery 1.10.2**

- o URL: <http://192.168.145.128/openemr/public/assets/jquery-datetimepicker/jquery.js>
- o Detection method: The library's name and version were determined based on the file's syntax fingerprint, and contents. Acunetix verified the library version and the associated vulnerabilities with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- o CVE-ID: CVE-2015-9251, CVE-2020-11022, CVE-2020-11023
- o Description: Possible Cross Site Scripting via third-party text/javascript responses / In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. / In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing option elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.
- o References:
  - <https://github.com/jquery/jquery/issues/2432>

- <http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/>
- <https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/>
- <https://mksben.l0.cm/2020/05/jquery3.5.0-xss.html>
- <https://jquery.com/upgrade-guide/3.5/>
- <https://api.jquery.com/jQuery.htmlPrefilter/>
- <https://www.cvedetails.com/cve/CVE-2020-11022/>
- <https://github.com/advisories/GHSA-gxr4-xjj5-5px2>
- <https://www.cvedetails.com/cve/CVE-2020-11023/>
- <https://github.com/advisories/GHSA-jpcq-cgw6-v4j6>

## Request

---

```
GET /openemr/public/assets/jquery-datetimepicker/jquery.js HTTP/1.1
Host: 192.168.145.128
accept: /*
accept-language: en-US
cookie: OpenEMR=SMoagLf26TS1Vx2PDvSGHTEJwG3t9eYeCWJyUPD7WNEu5a8X
Referer: http://192.168.145.128/openemr/public/assets/jquery-datetimepicker/
Accept-Encoding: gzip,deflate,br
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
```

<http://192.168.145.128/>

Verified

- **jQuery UI 1.8.10**

- URL: <http://192.168.145.128/openemr/interface/super/rules/www/js/cdr-multiselect/jquery-ui.min.js>
- Detection method: The library's name and version were determined based on the file's syntax fingerprint, and contents. Acunetix verified the library version and the associated vulnerabilities with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- CVE-ID: [CVE-2021-41184](#)
- Description: XSS in the 'of' option of the '.position()' util
- References:
  - <https://blog.jqueryui.com/2021/10/jquery-ui-1-13-0-released/>
  - <https://github.com/jquery/jquery-ui/security/advisories/GHSA-gpqq-952q-5327>

## Request

---

```
GET /openemr/interface/super/rules/www/js/cdr-multiselect/jquery-ui.min.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/interface/login_screen.php
Cookie: OpenEMR=2biStMm-fnsHdYMyYHQGKwzilsysHJvKUerLZszaOGdltFQQ
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
```

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)  
Chrome/109.0.0.0 Safari/537.36  
Host: 192.168.145.128  
Connection: Keep-alive

## <http://192.168.145.128/>

Verified

- **jQuery UI Dialog 1.8.10**

- URL: <http://192.168.145.128/openemr/interface/super/rules/www/js/cdr-multiselect/jquery-ui.min.js>
- Detection method: The library's name and version were determined based on the file's contents. Acunetix verified the library version and the associated vulnerabilities with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- CVE-ID: CVE-2010-5312, CVE-2016-7103
- Description: Title cross-site scripting vulnerability / XSS in dialog closeText
- References:
  - <http://bugs.jqueryui.com/ticket/6016>
  - <https://nodesecurity.io/advisories/127>
  - <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7103>
  - <https://www.cvedetails.com/cve/CVE-2016-7103/>

## Request

GET /openemr/interface/super/rules/www/js/cdr-multiselect/jquery-ui.min.js HTTP/1.1  
Acunetix-Aspect: enabled  
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7  
Acunetix-Aspect-ScanID: 1655702786608078775  
Acunetix-Aspect-Queries: aspectalerts;routes  
Referer: http://192.168.145.128/openemr/interface/login\_screen.php  
Cookie: OpenEMR=2biStMm-fnsHdYMyYHQGKwzilsysHJvKUerLZszaOGdltFQQ  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
Accept-Encoding: gzip,deflate,br  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)  
Chrome/109.0.0.0 Safari/537.36  
Host: 192.168.145.128  
Connection: Keep-alive

## <http://192.168.145.128/>

Verified

- **jQuery 1.5.1**

- URL: <http://192.168.145.128/openemr/interface/super/rules/www/js/cdr-multiselect/jquery.min.js>
- Detection method: The library's name and version were determined based on the file's syntax fingerprint, and contents. Acunetix verified the library version and the associated vulnerabilities with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- CVE-ID: CVE-2011-4969, CVE-2015-9251, CVE-2020-11022, CVE-2020-11023

- Description: Cross-site scripting (XSS) vulnerability in jQuery before 1.6.3, when using location.hash to select elements, allows remote attackers to inject arbitrary web script or HTML via a crafted tag. / Selector interpreted as HTML / Possible Cross Site Scripting via third-party text/javascript responses / In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. / In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing option elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.
- References:
  - <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4969>
  - <http://research.insecurelabs.org/jquery/test/>
  - <http://bugs.jquery.com/ticket/11290>
  - <https://github.com/jquery/jquery/issues/2432>
  - <http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/>
  - <https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/>
  - <https://mksben.l0.cm/2020/05/jquery3.5.0-xss.html>
  - <https://jquery.com/upgrade-guide/3.5/>
  - <https://api.jquery.com/jQuery.htmlPrefilter/>
  - <https://www.cvedetails.com/cve/CVE-2020-11022/>
  - <https://github.com/advisories/GHSA-gxr4-xjj5-px2>
  - <https://www.cvedetails.com/cve/CVE-2020-11023/>
  - <https://github.com/advisories/GHSA-jpcq-cgw6-v4j6>

## Request

---

```

GET /openemr/interface/super/rules/www/js/cdr-multiselect/jquery.min.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/interface/login_screen.php
Cookie: OpenEMR=2biStMm-fnsHdYMyYHQGKWzilsysHJvKUerLZszaOGdltFQQ
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
  
```

<http://192.168.145.128/>

Verified

- **jQuery 1.4.3**
  - URL: [http://192.168.145.128/openemr/interface/modules/zend\\_modules/public/js/lib/jquery.treeview-1.4.1/lib/jquery.js](http://192.168.145.128/openemr/interface/modules/zend_modules/public/js/lib/jquery.treeview-1.4.1/lib/jquery.js)

- Detection method: The library's name and version were determined based on the file's syntax fingerprint, and contents. Acunetix verified the library version and the associated vulnerabilities with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- CVE-ID: CVE-2011-4969, CVE-2015-9251, CVE-2020-11022, CVE-2020-11023
- Description: Cross-site scripting (XSS) vulnerability in jQuery before 1.6.3, when using location.hash to select elements, allows remote attackers to inject arbitrary web script or HTML via a crafted tag. / Selector interpreted as HTML / Possible Cross Site Scripting via third-party text/javascript responses / In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. / In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing option elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.
- References:
  - <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4969>
  - <http://research.insecurelabs.org/jquery/test/>
  - <http://bugs.jquery.com/ticket/11290>
  - <https://github.com/jquery/jquery/issues/2432>
  - <http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/>
  - <https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/>
  - <https://mksben.l0.cm/2020/05/jquery3.5.0-xss.html>
  - <https://jquery.com/upgrade-guide/3.5/>
  - <https://api.jquery.com/jQuery.htmlPrefilter/>
  - <https://www.cvedetails.com/cve/CVE-2020-11022/>
  - <https://github.com/advisories/GHSA-gxr4-xjj5-5px2>
  - <https://www.cvedetails.com/cve/CVE-2020-11023/>
  - <https://github.com/advisories/GHSA-jpcq-cgw6-v4j6>

## Request

---

```

GET /openemr/interface/modules/zend_modules/public/js/lib/jquery.treeview-1.4.1/lib/jquery.js
HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/interface/login_screen.php
Cookie: OpenEMR=2biStMm-fnsHdYMyYHQGKwzilsysHJvKUerLZszaOGdltFQQ
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive

```

<http://192.168.145.128/>

Verified

- **jQuery UI 1.11.4**

- URL: [http://192.168.145.128/openemr/interface/forms/eye\\_mag/js/jquery-ui-1-11-4/jquery-ui.min.js](http://192.168.145.128/openemr/interface/forms/eye_mag/js/jquery-ui-1-11-4/jquery-ui.min.js)
- Detection method: The library's name and version were determined based on the file's syntax fingerprint, and contents. Acunetix verified the library version and the associated vulnerabilities with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- CVE-ID: CVE-2021-41184
- Description: XSS in the 'of' option of the '.position()' util
- References:
  - <https://blog.jqueryui.com/2021/10/jquery-ui-1-13-0-released/>
  - <https://github.com/jquery/jquery-ui/security/advisories/GHSA-gpqq-952q-5327>

## Request

```
GET /openemr/interface/forms/eye_mag/js/jquery-ui-1-11-4/jquery-ui.min.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/interface/login_screen.php
Cookie: OpenEMR=2biStMm-fnsHdYMyYHQGKWzilsysHJvKUerLZszaOGdltFQQ
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

## <http://192.168.145.128/>

Verified

- **jQuery UI Dialog 1.11.4**

- URL: [http://192.168.145.128/openemr/interface/forms/eye\\_mag/js/jquery-ui-1-11-4/jquery-ui.min.js](http://192.168.145.128/openemr/interface/forms/eye_mag/js/jquery-ui-1-11-4/jquery-ui.min.js)
- Detection method: The library's name and version were determined based on the file's contents. Acunetix verified the library version and the associated vulnerabilities with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- CVE-ID: CVE-2016-7103
- Description: XSS in dialog closeText
- References:
  - <https://nodesecurity.io/advisories/127>
  - <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7103>
  - <https://www.cvedetails.com/cve/CVE-2016-7103/>

## Request

```
GET /openemr/interface/forms/eye_mag/js/jquery-ui-1-11-4/jquery-ui.min.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
```

Acunetix-Aspect-ScanID: 1655702786608078775  
Acunetix-Aspect-Queries: aspectalerts;routes  
Referer: http://192.168.145.128/openemr/interface/login\_screen.php  
Cookie: OpenEMR=2biStMm-fnsHdYMyYHQGKWzilsysHJvKUerLZszaOGdltFQQ  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
Accept-Encoding: gzip,deflate,br  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)  
Chrome/109.0.0.0 Safari/537.36  
Host: 192.168.145.128  
Connection: Keep-alive

## [http://192.168.145.128/](http://192.168.145.128)

Verified

- **jQuery 1.8.0**

- URL: [http://192.168.145.128/openemr/interface/modules/zend\\_modules/public/js/lib/jquery-1.8.0.min.js](http://192.168.145.128/openemr/interface/modules/zend_modules/public/js/lib/jquery-1.8.0.min.js)
- Detection method: The library's name and version were determined based on the file's name, and contents. Acunetix verified the library version and the associated vulnerabilities with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- CVE-ID: CVE-2015-9251, CVE-2020-11022, CVE-2020-11023
- Description: Selector interpreted as HTML / Possible Cross Site Scripting via third-party text/javascript responses / In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. / In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing option elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.
- References:
  - <http://bugs.jquery.com/ticket/11290>
  - <http://research.insecurelabs.org/jquery/test/>
  - <https://github.com/jquery/jquery/issues/2432>
  - <http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/>
  - <https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/>
  - <https://mksben.l0.cm/2020/05/jquery3.5.0-xss.html>
  - <https://jquery.com/upgrade-guide/3.5/>
  - <https://api.jquery.com/jQuery.htmlPrefilter/>
  - <https://www.cvedetails.com/cve/CVE-2020-11022/>
  - <https://github.com/advisories/GHSA-gxr4-xjj5-5px2>
  - <https://www.cvedetails.com/cve/CVE-2020-11023/>
  - <https://github.com/advisories/GHSA-jpcq-cgw6-v4j6>

## Request

---

```
GET /openemr/interface/modules/zend_modules/public/js/lib/jquery-1.8.0.min.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58adec3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
```

Acunetix-Aspect-Queries: aspectalerts;routes  
Referer: http://192.168.145.128/openemr/interface/login\_screen.php  
Cookie: OpenEMR=2biStMm-fnsHdYMyYHQGKwzilsysHJvKUerLZszaOGdltFQQ  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
Accept-Encoding: gzip,deflate,br  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)  
Chrome/109.0.0.0 Safari/537.36  
Host: 192.168.145.128  
Connection: Keep-alive

<http://192.168.145.128/>

Verified

- jQuery 1.8.2

- URL: http://192.168.145.128/openemr/interface/modules/zend\_modules/public/js/lib/jquery-1.8.2.min.js
- Detection method: The library's name and version were determined based on the file's name, and contents. Acunetix verified the library version and the associated vulnerabilities with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- CVE-ID: CVE-2015-9251, CVE-2020-11022, CVE-2020-11023
- Description: Selector interpreted as HTML / Possible Cross Site Scripting via third-party text/javascript responses / In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. / In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing option elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.
- References:
  - http://bugs.jquery.com/ticket/11290
  - http://research.insecurelabs.org/jquery/test/
  - https://github.com/jquery/jquery/issues/2432
  - http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/
  - https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/
  - https://mksben.lo.cm/2020/05/jquery3.5.0-xss.html
  - https://jquery.com/upgrade-guide/3.5/
  - https://api.jquery.com/jQuery.htmlPrefilter/
  - https://www.cvedetails.com/cve/CVE-2020-11022/
  - https://github.com/advisories/GHSA-gxr4-xjj5-5px2
  - https://www.cvedetails.com/cve/CVE-2020-11023/
  - https://github.com/advisories/GHSA-jpcq-cgw6-v4j6

## Request

GET /openemr/interface/modules/zend\_modules/public/js/lib/jquery-1.8.2.min.js HTTP/1.1  
Acunetix-Aspect: enabled  
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7  
Acunetix-Aspect-ScanID: 1655702786608078775  
Acunetix-Aspect-Queries: aspectalerts;routes

Referer: http://192.168.145.128/openemr/interface/login\_screen.php  
Cookie: OpenEMR=2biStMm-fnsHdYMyYHQGKwzilsysHJvKUerLZszaOGdltFQQ  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
Accept-Encoding: gzip,deflate,br  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)  
Chrome/109.0.0.0 Safari/537.36  
Host: 192.168.145.128  
Connection: Keep-alive

## <http://192.168.145.128/> Verified

- **jQuery 1.8.3**

- URL: [http://192.168.145.128/openemr/interface/modules/zend\\_modules/public/js/lib/jquery-1.8.3.js](http://192.168.145.128/openemr/interface/modules/zend_modules/public/js/lib/jquery-1.8.3.js)
- Detection method: The library's name and version were determined based on the file's name, and contents. Acunetix verified the library version and the associated vulnerabilities with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- CVE-ID: CVE-2015-9251, CVE-2020-11022, CVE-2020-11023
- Description: Selector interpreted as HTML / Possible Cross Site Scripting via third-party text/javascript responses / In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. / In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing option elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.
- References:
  - <http://bugs.jquery.com/ticket/11290>
  - <http://research.insecurelabs.org/jquery/test/>
  - <https://github.com/jquery/jquery/issues/2432>
  - <http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/>
  - <https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/>
  - <https://mksben.l0.cm/2020/05/jquery3.5.0-xss.html>
  - <https://jquery.com/upgrade-guide/3.5/>
  - <https://api.jquery.com/jQuery.htmlPrefilter/>
  - <https://www.cvedetails.com/cve/CVE-2020-11022/>
  - <https://github.com/advisories/GHSA-gxr4-xjj5-5px2>
  - <https://www.cvedetails.com/cve/CVE-2020-11023/>
  - <https://github.com/advisories/GHSA-jpcq-cgw6-v4j6>

## Request

---

```
GET /openemr/interface/modules/zend_modules/public/js/lib/jquery-1.8.3.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58adee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/interface/login_screen.php
```

Cookie: OpenEMR=2biStMm-fnsHdYMyYHQGKWzilsysHJvKUerLZszaOGdltFQQ  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
Accept-Encoding: gzip,deflate,br  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)  
Chrome/109.0.0.0 Safari/537.36  
Host: 192.168.145.128  
Connection: Keep-alive

## <http://192.168.145.128/>

Confidence: 80%

- **jQuery UI 1.9.2**

- URL: [http://192.168.145.128/openemr/interface/modules/zend\\_modules/public/js/lib/jquery-ui.custom.js](http://192.168.145.128/openemr/interface/modules/zend_modules/public/js/lib/jquery-ui.custom.js)
- Detection method: The library's name and version were determined based on the file's contents. Acunetix performed a syntax analysis of the file and detected functional differences between the file and the original library version. As the file was likely modified on purpose, the confidence level of the vulnerability alert has been lowered.
- CVE-ID: [CVE-2021-41184](#)
- Description: XSS in the 'of' option of the '.position()' util
- References:
  - <https://blog.jqueryui.com/2021/10/jquery-ui-1-13-0-released/>
  - <https://github.com/jquery/jquery-ui/security/advisories/GHSA-gpqq-952q-5327>

## Request

GET /openemr/interface/modules/zend\_modules/public/js/lib/jquery-ui.custom.js HTTP/1.1  
Acunetix-Aspect: enabled  
Acunetix-Aspect-Password: d4d608fef00a58adee3950d33ced68a7  
Acunetix-Aspect-ScanID: 1655702786608078775  
Acunetix-Aspect-Queries: aspectalerts;routes  
Referer: [http://192.168.145.128/openemr/interface/login\\_screen.php](http://192.168.145.128/openemr/interface/login_screen.php)  
Cookie: OpenEMR=2biStMm-fnsHdYMyYHQGKWzilsysHJvKUerLZszaOGdltFQQ  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
Accept-Encoding: gzip,deflate,br  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)  
Chrome/109.0.0.0 Safari/537.36  
Host: 192.168.145.128  
Connection: Keep-alive

## <http://192.168.145.128/>

Confidence: 95%

- **jQuery UI Datepicker 1.9.2**

- URL: [http://192.168.145.128/openemr/interface/modules/zend\\_modules/public/js/lib/jquery-ui.custom.js](http://192.168.145.128/openemr/interface/modules/zend_modules/public/js/lib/jquery-ui.custom.js)
- Detection method: The library's name and version were determined based on the file's contents.
- CVE-ID: [CVE-2021-41182](#), [CVE-2021-41183](#)

- Description: XSS in the 'altField' option of the Datepicker widget / XSS in '\*Text' options of the Datepicker widget
- References:
  - <https://blog.jqueryui.com/2021/10/jquery-ui-1-13-0-released/>
  - <https://github.com/jquery/jquery-ui/security/advisories/GHSA-9gj3-hwp5-pmwc>
  - <https://github.com/jquery/jquery-ui/security/advisories/GHSA-j7qv-pgf6-hvh4>

## Request

---

```
GET /openemr/interface/modules/zend_modules/public/js/lib/jquery-ui.custom.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/interface/login_screen.php
Cookie: OpenEMR=2biStMm-fnsHdYMyYHQGKwzilsysHJvKUerLZszaOGdltFQQ
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

## <http://192.168.145.128/>

Verified

- **jQuery UI 1.10.3**
  - URL: [http://192.168.145.128/openemr/interface/modules/zend\\_modules/public/js/lib/jquery-ui.js](http://192.168.145.128/openemr/interface/modules/zend_modules/public/js/lib/jquery-ui.js)
  - Detection method: The library's name and version were determined based on the file's syntax fingerprint, and contents. Acunetix verified the library version and the associated vulnerabilities with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
  - CVE-ID: CVE-2021-41184
  - Description: XSS in the 'of' option of the '.position()' util
  - References:
    - <https://blog.jqueryui.com/2021/10/jquery-ui-1-13-0-released/>
    - <https://github.com/jquery/jquery-ui/security/advisories/GHSA-gpqq-952q-5327>

## Request

---

```
GET /openemr/interface/modules/zend_modules/public/js/lib/jquery-ui.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/interface/login_screen.php
Cookie: OpenEMR=2biStMm-fnsHdYMyYHQGKwzilsysHJvKUerLZszaOGdltFQQ
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
```

Chrome/109.0.0.0 Safari/537.36

Host: 192.168.145.128

Connection: Keep-alive

**http://192.168.145.128/**

Verified

- **jQuery UI Dialog 1.10.3**

- URL: http://192.168.145.128/openemr/interface/modules/zend\_modules/public/js/lib/jquery-ui.js
- Detection method: The library's name and version were determined based on the file's contents. Acunetix verified the library version and the associated vulnerabilities with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- CVE-ID: CVE-2016-7103
- Description: XSS in dialog closeText
- References:
  - <https://nodesecurity.io/advisories/127>
  - <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7103>
  - <https://www.cvedetails.com/cve/CVE-2016-7103/>

## Request

```
GET /openemr/interface/modules/zend_modules/public/js/lib/jquery-ui.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/interface/login_screen.php
Cookie: OpenEMR=2biStMm-fnsHdYMyYHQGKWzilsysHJvKUerLZszaOGdltFQQ
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

**http://192.168.145.128/**

Confidence: 95%

- **jQuery UI Datepicker 1.10.3**

- URL: http://192.168.145.128/openemr/interface/modules/zend\_modules/public/js/lib/jquery-ui.js
- Detection method: The library's name and version were determined based on the file's contents.
- CVE-ID: CVE-2021-41182, CVE-2021-41183
- Description: XSS in the 'altField' option of the Datepicker widget / XSS in '\*Text' options of the Datepicker widget
- References:
  - <https://blog.jqueryui.com/2021/10/jquery-ui-1-13-0-released/>

- <https://github.com/jquery/jquery-ui/security/advisories/GHSA-9gj3-hwp5-pmw>
- <https://github.com/jquery/jquery-ui/security/advisories/GHSA-j7qv-pgf6-hvh4>

## Request

---

```
GET /openemr/interface/modules/zend_modules/public/js/lib/jquery-ui.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/interface/login_screen.php
Cookie: OpenEMR=2biStMm-fnsHdYMyYHQGKWzilsysHJvKUerLZszaOGdltFQQ
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

## Recommendation

---

Upgrade to the latest version.

## Vulnerable package dependencies [medium]

---

One or more packages that are used in your web application are affected by known vulnerabilities. Please consult the details section for more information about each affected package.

### CWE

CWE-1104

## Impact

---

The impact of this vulnerability is different for each vulnerable package. It's recommended to investigate each vulnerable package individually.

## <http://10.10.236.31/openemr/>

List of vulnerable **composer** packages:

**Package:** dompdf/dompdf

**Version:** 1.2.2

**CVE:** CVE-2022-0085

**Title:** Server-Side Request Forgery (SSRF)

**Description:** Server-Side Request Forgery (SSRF) in GitHub repository dompdf/dompdf prior to 2.0.0.

**CVSS V2:** AV:N/AC:M/Au:N/C:N/I:P/A:N

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

**CWE:** CWE-918

**References:**

- <https://github.com/dompdf/dompdf/commit/bb1ef65011a14730b7cfbe73506b4bb8a03704bd>
- <https://huntr.dev/bounties/73dbcc78-5ba9-492f-9133-13bbc9f31236>

**Package:** dompdf/dompdf

**Version:** 1.2.2

**CVE:** CVE-2022-2400

**Title:** External Control of File Name or Path

**Description:** External Control of File Name or Path in GitHub repository dompdf/dompdf prior to 2.0.0.

**CVSS V2:**

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

**CWE:** CWE-73

**References:**

- <https://huntr.dev/bounties/a6da5e5e-86be-499a-a3c3-2950f749202a>
- <https://github.com/dompdf/dompdf/commit/99aeec1efec9213e87098d42eb09439e7ee0bb6a>

**Package:** smarty/smarty

**Version:** 2.6.33

**CVE:** CVE-2018-16831

**Title:** Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

**Description:** Smarty before 3.1.33-dev-4 allows attackers to bypass the trusted\_dir protection mechanism via a file:../../ substring in an include statement.

**CVSS V2:** AV:N/AC:M/Au:N/C:C/I:N/A:N

**CVSS V3:** CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N

**CWE:** CWE-22

**References:**

- <https://github.com/smarty-php/smarty/issues/486>

**Package:** smarty/smarty

**Version:** 2.6.33

**CVE:** CVE-2018-25047

**Title:** Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

**Description:** In Smarty before 3.1.47 and 4.x before 4.2.1, libs/plugins/function.mailto.php allows XSS. A web page that uses smarty\_function\_mailto, and that could be parameterized using GET or POST input parameters, could allow injection of JavaScript code by a user.

**CVSS V2:**

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N

**CWE:** CWE-79

**References:**

- <https://github.com/smarty-php/smarty/releases/tag/v4.2.1>
- <https://github.com/smarty-php/smarty/releases/tag/v3.1.47>
- <https://bugs.gentoo.org/870100>

- <https://github.com/smarty-php/smarty/issues/454>
- <https://security.gentoo.org/glsa/202209-09>
- <https://lists.debian.org/debian-lts-announce/2023/01/msg00002.html>

**Package:** smarty/smarty

**Version:** 2.6.33

**CVE:** CVE-2023-28447

**Title:** Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

**Description:** Smarty is a template engine for PHP. In affected versions smarty did not properly escape javascript code. An attacker could exploit this vulnerability to execute arbitrary JavaScript code in the context of the user's browser session. This may lead to unauthorized access to sensitive user data, manipulation of the web application's behavior, or unauthorized actions performed on behalf of the user. Users are advised to upgrade to either version 3.1.48 or to 4.3.1 to resolve this issue. There are no known workarounds for this vulnerability.

**CVSS V2:**

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

**CWE:** CWE-79

**References:**

- <https://github.com/smarty-php/smarty/security/advisories/GHSA-7j98-h7fp-4vwj>
- <https://github.com/smarty-php/smarty/commit/685662466f653597428966d75a661073104d713d>

## <http://192.168.145.128/openemr/>

List of vulnerable **composer** packages:

**Package:** dompdf/dompdf

**Version:** 1.2.2

**CVE:** CVE-2022-0085

**Title:** Server-Side Request Forgery (SSRF)

**Description:** Server-Side Request Forgery (SSRF) in GitHub repository dompdf/dompdf prior to 2.0.0.

**CVSS V2:** AV:N/AC:M/Au:N/C:N/I:P/A:N

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

**CWE:** CWE-918

**References:**

- <https://github.com/dompdf/dompdf/commit/bb1ef65011a14730b7cfbe73506b4bb8a03704bd>
- <https://huntr.dev/bounties/73dbcc78-5ba9-492f-9133-13bbc9f31236>

**Package:** dompdf/dompdf

**Version:** 1.2.2

**CVE:** CVE-2022-2400

**Title:** External Control of File Name or Path

**Description:** External Control of File Name or Path in GitHub repository dompdf/dompdf prior to 2.0.0.

**CVSS V2:**

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

**CWE:** CWE-73

**References:**

- <https://huntr.dev/bounties/a6da5e5e-86be-499a-a3c3-2950f749202a>
- <https://github.com/dompdf/dompdf/commit/99aec1efec9213e87098d42eb09439e7ee0bb6a>

**Package:** smarty/smarty

**Version:** 2.6.33

**CVE:** CVE-2018-16831

**Title:** Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

**Description:** Smarty before 3.1.33-dev-4 allows attackers to bypass the trusted\_dir protection mechanism via a file:../ substring in an include statement.

**CVSS V2:** AV:N/AC:M/Au:N/C:C/I:N/A:N

**CVSS V3:** CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N

**CWE:** CWE-22

**References:**

- <https://github.com/smarty-php/smarty/issues/486>

**Package:** smarty/smarty

**Version:** 2.6.33

**CVE:** CVE-2018-25047

**Title:** Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

**Description:** In Smarty before 3.1.47 and 4.x before 4.2.1, libs/plugins/function.mailto.php allows XSS. A web page that uses smarty\_function\_mailto, and that could be parameterized using GET or POST input parameters, could allow injection of JavaScript code by a user.

**CVSS V2:**

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N

**CWE:** CWE-79

**References:**

- <https://github.com/smarty-php/smarty/releases/tag/v4.2.1>
- <https://github.com/smarty-php/smarty/releases/tag/v3.1.47>
- <https://bugs.gentoo.org/870100>
- <https://github.com/smarty-php/smarty/issues/454>
- <https://security.gentoo.org/glsa/202209-09>
- <https://lists.debian.org/debian-lts-announce/2023/01/msg00002.html>

**Package:** smarty/smarty

**Version:** 2.6.33

**CVE:** CVE-2023-28447

**Title:** Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

**Description:** Smarty is a template engine for PHP. In affected versions smarty did not properly escape javascript code. An attacker could exploit this vulnerability to execute arbitrary JavaScript code in the context of the user's browser session. This may lead to unauthorized access to sensitive user data, manipulation of the web application's behavior, or

Unauthorized actions performed on behalf of the user. Users are advised to upgrade to either version 3.1.48 or to 4.3.1 to resolve this issue. There are no known workarounds for this vulnerability.

#### CVSS V2:

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

**CWE:** CWE-79

#### References:

- <https://github.com/smarty-php/smarty/security/advisories/GHSA-7j98-h7fp-4vwj>
- <https://github.com/smarty-php/smarty/commit/685662466f653597428966d75a661073104d713d>

## Recommendation

It's recommended to update the vulnerable packages to the latest version (if a fix exists). If a fix does not exist, you may want to suggest changes that address the vulnerability to the package maintainer or remove the package from your dependency tree.

## Outdated JavaScript libraries

You are using an outdated version of one or more JavaScript libraries. A more recent version is available. Although your version was not found to be affected by any security vulnerabilities, it is recommended to keep libraries up to date.

#### CWE

CWE-937

#### CVSS2

AV:N/AC:H/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	High
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

#### CVSS3

CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	High
Privileges Required	None
User Interaction	Required
Scope	Changed
Confidentiality	None
Integrity Impact	None
Availability Impact	None

## Impact

Consult References for more information.

<http://10.10.236.31/>

Verified

- **jQuery UI Dialog 1.12.1**

- URL: <http://10.10.236.31/openemr/public/assets/jquery-ui/jquery-ui.js>
- Detection method: The library's name and version were determined based on the file's contents. Acunetix verified the library version with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- References:
  - <https://jqueryui.com/download/>

## Request

```
GET /openemr/public/assets/jquery-ui/jquery-ui.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 8595e182db21cbbc10c83c2c4cf193d3
Acunetix-Aspect-ScanID: 816589585389164376
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://10.10.236.31/openemr/Documentation/help_files/openemr_installation_help.php
Cookie: OpenEMR=b3DHM9s5BR72IjC3y6GcpBb736abtMj3%2CfzaSNeoS-j94pMx
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 10.10.236.31
Connection: Keep-alive
```

<http://10.10.236.31/>

Verified

- **jQuery UI Tooltip 1.12.1**

- URL: <http://10.10.236.31/openemr/public/assets/jquery-ui/jquery-ui.js>
- Detection method: The library's name and version were determined based on the file's contents. Acunetix verified the library version with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- References:
  - <https://jqueryui.com/download/>

## Request

```
GET /openemr/public/assets/jquery-ui/jquery-ui.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 8595e182db21cbbc10c83c2c4cf193d3
Acunetix-Aspect-ScanID: 816589585389164376
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://10.10.236.31/openemr/Documentation/help_files/openemr_installation_help.php
Cookie: OpenEMR=b3DHM9s5BR72IjC3y6GcpBb736abtMj3%2CfzaSNeoS-j94pMx
```

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
Accept-Encoding: gzip,deflate,br  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)  
Chrome/109.0.0.0 Safari/537.36  
Host: 10.10.236.31  
Connection: Keep-alive

## <http://192.168.145.128/>

Verified

- **jQuery UI Dialog 1.12.1**

- URL: <http://192.168.145.128/openemr/public/assets/jquery-ui/jquery-ui.js>
- Detection method: The library's name and version were determined based on the file's contents. Acunetix verified the library version with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- References:
  - <https://jqueryui.com/download/>

## Request

```
GET /openemr/public/assets/jquery-ui/jquery-ui.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/Documentation/help_files/openemr_installation_help.php
Cookie: OpenEMR=d40D5DeYlSqGsuSImcMvd1XbnUvSB1Sl%2CNIItqLcdHnpIKp4G
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

## <http://192.168.145.128/>

Verified

- **jQuery UI Tooltip 1.12.1**

- URL: <http://192.168.145.128/openemr/public/assets/jquery-ui/jquery-ui.js>
- Detection method: The library's name and version were determined based on the file's contents. Acunetix verified the library version with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- References:
  - <https://jqueryui.com/download/>

## Request

```
GET /openemr/public/assets/jquery-ui/jquery-ui.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58ad3e3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/Documentation/help_files/openemr_installation_help.php
Cookie: OpenEMR=d4D5DeY1SqGsuSImcMvd1XbnUvSB1S1%2CNItgLcdHnpIKp4G
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

## <http://192.168.145.128/>

Verified

- **jQuery UI Tooltip 1.11.4**

- URL: [http://192.168.145.128/openemr/interface/forms/eye\\_mag/js/jquery-ui-1-11-4/jquery-ui.min.js](http://192.168.145.128/openemr/interface/forms/eye_mag/js/jquery-ui-1-11-4/jquery-ui.min.js)
- Detection method: The library's name and version were determined based on the file's contents. Acunetix verified the library version with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- References:
  - <https://jqueryui.com/download/>

## Request

```
GET /openemr/interface/forms/eye_mag/js/jquery-ui-1-11-4/jquery-ui.min.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58ad3e3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/interface/login_screen.php
Cookie: OpenEMR=2biStMm-fnsHdYMyYHQGKwzilsysHJvKUerLZszaOGdltFQQ
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

## <http://192.168.145.128/>

Verified

- **jQuery UI Tooltip 1.10.3**

- URL: [http://192.168.145.128/openemr/interface/modules/zend\\_modules/public/js/lib/jquery-ui.js](http://192.168.145.128/openemr/interface/modules/zend_modules/public/js/lib/jquery-ui.js)
- Detection method: The library's name and version were determined based on the file's contents. Acunetix verified the library version with the file's unique syntax fingerprint, which matched the syntax fingerprint

expected by Acunetix.

- o References:

- <https://jqueryui.com/download/>

## Request

---

```
GET /openemr/interface/modules/zend_modules/public/js/lib/jquery-ui.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/interface/login_screen.php
Cookie: OpenEMR=2biStMm-fnsHdYMyYHQGKWzilsysHJvKUerLZszaOGdltFQQ
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

## <http://192.168.145.128/>

Confidence: 95%

- Modernizr 2.6.2

- o URL: [http://192.168.145.128/openemr/interface/modules/zend\\_modules/public/js/lib/modernizr-2.6.2.min.js](http://192.168.145.128/openemr/interface/modules/zend_modules/public/js/lib/modernizr-2.6.2.min.js)
  - o Detection method: The library's name and version were determined based on the file's name.
  - o References:
    - <https://github.com/Modernizr/Modernizr/releases>

## Request

---

```
GET /openemr/interface/modules/zend_modules/public/js/lib/modernizr-2.6.2.min.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/interface/login_screen.php
Cookie: OpenEMR=2biStMm-fnsHdYMyYHQGKWzilsysHJvKUerLZszaOGdltFQQ
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

## Recommendation

---

Upgrade to the latest version.

## PHP allow\_url\_fopen enabled

---

The PHP configuration directive allow\_url\_fopen is enabled. When enabled, this directive allows data retrieval from remote locations (web site or FTP server). A large number of code injection vulnerabilities reported in PHP-based web applications are caused by the combination of enabling allow\_url\_fopen and bad input filtering.

allow\_url\_fopen is enabled by default.

### CWE

CWE-829

### CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

### CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Changed
Confidentiality	None
Integrity Impact	None
Availability Impact	None

## Impact

---

Application dependant - possible remote file inclusion.

<http://10.10.236.31/>



Verified

Current setting is : **allow\_url\_fopen = on**

Observed on /openemr/interface/product\_registration/product\_registration\_controller.php

<http://192.168.145.128/>



Verified

Current setting is : **allow\_url\_fopen = on**

Observed on /openemr/interface/main/main\_screen.php

## Recommendation

---

You can disable allow\_url\_fopen from either php.ini (for PHP versions newer than 4.3.4) or .htaccess (for PHP versions up to 4.3.4).

#### php.ini

```
allow_url_fopen = 'off'
```

#### .htaccess

```
php_flag allow_url_fopen off
```

## References

---

### [Runtime Configuration](#)

<https://www.php.net/manual/en/filesystem.configuration.php>

## Directory listings

---

Directory listing is a web server function that displays the directory contents when there is no index file in a specific website directory. It is dangerous to leave this function turned on for the web server because it leads to information disclosure.

### CWE

CWE-538

### CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

### CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

## Impact

---

A user can view a list of all files from the affected directories possibly exposing sensitive information.

<http://10.10.236.31/>

Verified

Folders with directory listing enabled:

- http://10.10.236.31/openemr/interface/
- http://10.10.236.31/openemr/interface/login/
- http://10.10.236.31/openemr/public/assets/moment/min/
- http://10.10.236.31/openemr/public/assets/knockout/build/output/
- http://10.10.236.31/openemr/public/
- http://10.10.236.31/openemr/interface/main/
- http://10.10.236.31/openemr/public/assets/i18next/dist/umd/
- http://10.10.236.31/openemr/public/assets/knockout/
- http://10.10.236.31/openemr/public/assets/knockout/build/
- http://10.10.236.31/openemr/library/js/
- http://10.10.236.31/openemr/Documentation/
- http://10.10.236.31/openemr/Documentation/help\_files/
- http://10.10.236.31/openemr/public/assets/hotkeys-js/
- http://10.10.236.31/openemr/public/assets/hotkeys-js/dist/
- http://10.10.236.31/openemr/library/js/vendors/
- http://10.10.236.31/openemr/library/js/vendors/validate/
- http://10.10.236.31/openemr/public/assets/jquery-datetimepicker/build/
- http://10.10.236.31/openemr/interface/main/messages/css/
- http://10.10.236.31/openemr/public/assets/jquery/
- http://10.10.236.31/openemr/interface/main/dated\_reminders/
- http://10.10.236.31/openemr/interface/product\_registration/

## Request

---

```
GET /openemr/interface/ HTTP/1.1
Cookie: OpenEMR=bbs80gzIFbvo7hR%2Cj5ZvMq%2C3QTQmauASLmo3p3YX9WgoZJp2
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 10.10.236.31
Connection: Keep-alive
```

## <http://192.168.145.128/>

Verified

Folders with directory listing enabled:

- http://192.168.145.128/openemr/interface/
- http://192.168.145.128/openemr/interface/login/
- http://192.168.145.128/openemr/interface/main/messages/css/
- http://192.168.145.128/openemr/public/assets/
- http://192.168.145.128/openemr/public/assets/bootstrap/dist/js/
- http://192.168.145.128/openemr/interface/main/messages/js/
- http://192.168.145.128/openemr/public/assets/moment/

- <http://192.168.145.128/openemr/library/ajax/>
- [http://192.168.145.128/openemr/interface/main/dated\\_reminders/](http://192.168.145.128/openemr/interface/main/dated_reminders/)
- <http://192.168.145.128/openemr/public/assets/select2/dist/css/>
- <http://192.168.145.128/openemr/public/assets/moment/min/>
- [http://192.168.145.128/openemr/interface/product\\_registration/](http://192.168.145.128/openemr/interface/product_registration/)
- <http://192.168.145.128/openemr/Documentation/>
- <http://192.168.145.128/openemr/public/assets/bootstrap/dist/>
- <http://192.168.145.128/openemr/interface/main/tabs/js/>
- <http://192.168.145.128/openemr/public/assets/i18next/dist/>
- <http://192.168.145.128/openemr/public/assets/i18next/dist/umd/>
- <http://192.168.145.128/openemr/public/>
- <http://192.168.145.128/openemr/public/assets/i18next/>
- <http://192.168.145.128/openemr/public/assets/knockout/>
- <http://192.168.145.128/openemr/public/assets/hotkeys-js/dist/>

## Request

---

```
GET /openemr/interface/ HTTP/1.1
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

## Recommendation

---

You should make sure no sensitive information is disclosed or you may want to restrict directory listings from the web server configuration.

## Description

---

### How to disable directory listings

The easiest way to disable directory listing is to create an index file. The name of the index file depends on the web server configuration. On Apache is called index.htm, index.html. On IIS is named default.asp, default.aspx, default.htm.

On IIS directory listings are disabled by default.

For Apache you need to edit the Apache configuration file (usually named httpd.conf) or create an .htaccess file. In the configuration file you will have the definition of the directory. Something like

```
<Directory /directoryname/subdirectory> Options Indexes FollowSymLinks ...
</Directory>
```

To disable directory listing for that directory you need to remove the 'Indexes' option.

## References

---

## PHP open\_basedir is not set

The open\_basedir configuration directive will limit the files that can be opened by PHP to the specified directory-tree. When a script tries to open a file with, for example, fopen() or gzopen(), the location of the file is checked. When the file is outside the specified directory-tree, PHP will refuse to open it. open\_basedir is a good protection against remote file inclusion vulnerabilities. For a remote attacker it is not possible to break out of the open\_basedir restrictions if he is only able to inject the name of a file to be included. Therefore the number of files he will be able to include with such a local file include vulnerability is limited.

### CWE

CWE-664

### CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

### CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Changed
Confidentiality	None
Integrity Impact	None
Availability Impact	None

## Impact

Application dependant - possible remote code inclusion.

<http://10.10.236.31/>



Verified

Current setting is : `open_basedir=`

Observed on /openemr/interface/product\_registration/product\_registration\_controller.php

<http://192.168.145.128/>



Verified

Current setting is : `open_basedir=`

Observed on /openemr/interface/main/main\_screen.php

## Recommendation

You can set open\_basedir from php.ini

### php.ini

open\_basedir = your\_application\_directory

## Cookies without HttpOnly flag set

One or more cookies don't have the HttpOnly flag set. When a cookie is set with the HttpOnly flag, it instructs the browser that the cookie can only be accessed by the server and not by client-side scripts. This is an important security protection for session cookies.

### CWE

CWE-1004

### CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

### CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Unchanged
Confidentiality	None
Integrity Impact	None
Availability Impact	None

## Impact

Cookies can be accessed by client-side scripts.

<http://10.10.236.31/>

Verified

Cookies without HttpOnly flag set:

- http://10.10.236.31/openemr/interface/main/main\_screen.php

Set-Cookie: OpenEMR=LmmZhzcLsqldB4AesxJ%2CR%2Cq%2C%2CrGBXmlKjWUU8woh9PdRSK79; path=/openemr/; SameSite=Strict

Set-Cookie: OpenEMR=Dj68HNoGw-vYWT2k81NHDiqIHhLtrgfoVY0Tqo%2Cj6JeJm5aU; path=/openemr/; SameSite=Strict

- <http://10.10.236.31/openemr/interface/login/login.php>

Set-Cookie: OpenEMR=8Z13vTsN2fHQEa1Rcsk139L%2CqHc8NRZ%2CasvpnHWgLB8JHmW2; path=/openemr/; SameSite=Strict

- <http://10.10.236.31/openemr/interface/main/calendar/index.php>

Set-Cookie: OpenEMR=Dj68HNoGw-vYWT2k81NHDiqIHhLtrgfoVY0Tqo%2Cj6JeJm5aU; path=/openemr/; SameSite=Strict

- <http://10.10.236.31/openemr/interface/main/calendar/>

Set-Cookie: OpenEMR=bbs8OgzIFbvo7hR%2Cj5ZvMq%2C3QTQmauASLmo3p3YX9WgoZJp2; path=/openemr/; SameSite=Strict

- [http://10.10.236.31/openemr/library/ajax/dated\\_reminders\\_counter.php](http://10.10.236.31/openemr/library/ajax/dated_reminders_counter.php)

Set-Cookie: OpenEMR=Dj68HNoGw-vYWT2k81NHDiqIHhLtrgfoVY0Tqo%2Cj6JeJm5aU; path=/openemr/; SameSite=Strict

- <http://10.10.236.31/openemr/interface/main/calendar/index.php>

Set-Cookie: OpenEMR=Dj68HNoGw-vYWT2k81NHDiqIHhLtRgfoVY0Tqo%2Cj6JeJm5aU; path=/openemr/; SameSite=Strict

- <http://10.10.236.31/openemr/interface/main/tabs/main.php>

Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/openemr/; SameSite=Strict

- <http://10.10.236.31/openemr/portal/messaging/messages.php>

Set-Cookie: OpenEMR=t8OBJqr%2C0IVS5N1iDb%2CwppNgQ0K3h5UOCm1n0u5jQeS8WoRL; path=/openemr/; SameSite=Strict

- [http://10.10.236.31/openemr/portal/messaging/secure\\_chat.php](http://10.10.236.31/openemr/portal/messaging/secure_chat.php)

Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/openemr/; SameSite=Strict

- [http://10.10.236.31/openemr/Documentation/help\\_files/add\\_edit\\_transactions\\_dashboard\\_help.php](http://10.10.236.31/openemr/Documentation/help_files/add_edit_transactions_dashboard_help.php)

Set-Cookie: OpenEMR=VLl7hzvLG07yM4KXKZmRPAlPreAFCwPCOs83wZc1Rq78Z-kv; path=/openemr/; SameSite=Strict

- [http://10.10.236.31/openemr/library/ajax/execute\\_background\\_services.php](http://10.10.236.31/openemr/library/ajax/execute_background_services.php)

Set-Cookie: OpenEMR=hudaHjq4SnRX1Fop74MFMPiFIyrvFv9YoXaoUOukTQd1tTJV; path=/openemr/; SameSite=Strict

- [http://10.10.236.31/openemr/Documentation/help\\_files/adminacl\\_help.php](http://10.10.236.31/openemr/Documentation/help_files/adminacl_help.php)

Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/openemr/; SameSite=Strict

- [http://10.10.236.31/openemr/Documentation/help\\_files/cms\\_1500\\_help.php](http://10.10.236.31/openemr/Documentation/help_files/cms_1500_help.php)

Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/openemr/; SameSite=Strict

- [http://10.10.236.31/openemr/Documentation/help\\_files/common\\_help.php](http://10.10.236.31/openemr/Documentation/help_files/common_help.php)

Set-Cookie: OpenEMR=EnR3PUdKNldPyhV%2CwLu8RKtyTDZpjpfVW7tWlfIccceAnhI; path=/openemr/; SameSite=Strict

- [http://10.10.236.31/openemr/Documentation/help\\_files/configure\\_orders\\_help.php](http://10.10.236.31/openemr/Documentation/help_files/configure_orders_help.php)

Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/openemr/; SameSite=Strict

- [http://10.10.236.31/openemr/library/ajax/imm\\_autocomplete/search.php](http://10.10.236.31/openemr/library/ajax/imm_autocomplete/search.php)

Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/openemr/; SameSite=Strict

- [http://10.10.236.31/openemr/Documentation/help\\_files/cqm\\_amc\\_help.php](http://10.10.236.31/openemr/Documentation/help_files/cqm_amc_help.php)

Set-Cookie: OpenEMR=pdOa1VLshTozyApH8zNI2d7HnUwIONZy3q2UoD4%2C09b18v37; path=/openemr/; SameSite=Strict

- <http://10.10.236.31/openemr/library/ajax/addlistitem.php>

Set-Cookie: OpenEMR=ioj%2CUPnhPA4t-uwiHKvT2oLoWeqJyJrdV-zbtKJBgRWmOht3; path=/openemr/; SameSite=Strict

- [http://10.10.236.31/openemr/Documentation/help\\_files/fee\\_sheet\\_help.php](http://10.10.236.31/openemr/Documentation/help_files/fee_sheet_help.php)

Set-Cookie: OpenEMR=HGgNew%2C6C617YxcKHIQ1jyGaWExaE6FIX%2Cc7zDwiT%2C8zvYzG; path=/openemr/; SameSite=Strict

- [http://10.10.236.31/openemr/library/ajax/adminacl\\_ajax.php](http://10.10.236.31/openemr/library/ajax/adminacl_ajax.php)

```
Set-Cookie: OpenEMR=1TJQMuK6TLzv79W4QvnA42eBiDDj0r5dbf4fTI%2Cy72rMHGzt;  
path=/openemr/; SameSite=Strict
```

- [http://10.10.236.31/openemr/Documentation/help\\_files/mfa\\_help.php](http://10.10.236.31/openemr/Documentation/help_files/mfa_help.php)

```
Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0;  
path=/openemr/; SameSite=Strict
```

## Request

---

```
POST /openemr/interface/main/main_screen.php?auth=login&site=default HTTP/1.1  
Host: 10.10.236.31  
Content-Length: 119  
Pragma: no-cache  
Cache-Control: no-cache  
Upgrade-Insecure-Requests: 1  
Origin: http://10.10.236.31  
Content-Type: application/x-www-form-urlencoded  
Accept-Language: en-US  
Accept:  
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9  
Referer: http://10.10.236.31/openemr/interface/login/login.php?site=default  
Accept-Encoding: gzip,deflate,br  
Connection: keep-alive  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)  
Chrome/109.0.0.0 Safari/537.36  
  
new_login_session_management=1&languageChoice=1&authUser=openemr_carlos_mejia&clearPass=Climcrisnaya  
3*&languageChoice=1
```

## <http://192.168.145.128/>

Verified

Cookies without HttpOnly flag set:

- <http://192.168.145.128/openemr/interface/login/login.php>

```
Set-Cookie: OpenEMR=PrCCihxJI%2CqG1CXOp7oP16LOkuij2mG5Yq0pHL59ThbnUpzb;  
path=/openemr/; SameSite=Strict
```

- [http://192.168.145.128/openemr/library/ajax/dated\\_reminders\\_counter.php](http://192.168.145.128/openemr/library/ajax/dated_reminders_counter.php)

Set-Cookie: OpenEMR=fLVw-dnCSU123MMDJ4XDEmokIFFZN%2CUpA0oNxhYRlFnqazp; path=/openemr/; SameSite=Strict

- <http://192.168.145.128/openemr/interface/main/calendar/index.php>

Set-Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15; path=/openemr/; SameSite=Strict

- <http://192.168.145.128/openemr/interface/main/calendar/index.php>

Set-Cookie: OpenEMR=fLVw-dnCSU123MMDJ4XDEmokIFFZN%2CUpA0oNxhYRlFnqazp; path=/openemr/; SameSite=Strict

- [http://192.168.145.128/openemr/interface/main/main\\_screen.php](http://192.168.145.128/openemr/interface/main/main_screen.php)

Set-Cookie: OpenEMR=9Y8ac4csy6RvRyifO9Yg1001but4qLPoxBtXKUc8Kxsv0A5J; path=/openemr/; SameSite=Strict

- <http://192.168.145.128/openemr/interface/main/tabs/main.php>

Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/openemr/; SameSite=Strict

- <http://192.168.145.128/openemr/portal/messaging/messages.php>

Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/openemr/; SameSite=Strict

- [http://192.168.145.128/openemr/portal/messaging/secure\\_chat.php](http://192.168.145.128/openemr/portal/messaging/secure_chat.php)

Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/openemr/; SameSite=Strict

- [http://192.168.145.128/openemr/Documentation/help\\_files/add\\_edit\\_transactions\\_dashboard\\_help.php](http://192.168.145.128/openemr/Documentation/help_files/add_edit_transactions_dashboard_help.php)

Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/openemr/; SameSite=Strict

- [http://192.168.145.128/openemr/library/ajax/execute\\_background\\_services.php](http://192.168.145.128/openemr/library/ajax/execute_background_services.php)

Set-Cookie: OpenEMR=W75Ms9wo0idBaU3cwZ3komU0jWJ6XL2Pyzz3muoDQyhZHx; path=/openemr/; SameSite=Strict

- [http://192.168.145.128/openemr/Documentation/help\\_files/adminacl\\_help.php](http://192.168.145.128/openemr/Documentation/help_files/adminacl_help.php)

Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/openemr/; SameSite=Strict

- [http://192.168.145.128/openemr/Documentation/help\\_files/cms\\_1500\\_help.php](http://192.168.145.128/openemr/Documentation/help_files/cms_1500_help.php)

Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/openemr/; SameSite=Strict

- <http://192.168.145.128/openemr/library/FeeSheet.class.php>

Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/openemr/; SameSite=Strict

- [http://192.168.145.128/openemr/Documentation/help\\_files/common\\_help.php](http://192.168.145.128/openemr/Documentation/help_files/common_help.php)

Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/openemr/; SameSite=Strict

- <http://192.168.145.128/openemr/library/FeeSheetHtml.class.php>

Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/openemr/; SameSite=Strict

- [http://192.168.145.128/openemr/Documentation/help\\_files/configure\\_orders\\_help.php](http://192.168.145.128/openemr/Documentation/help_files/configure_orders_help.php)

Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/openemr/; SameSite=Strict

- [http://192.168.145.128/openemr/Documentation/help\\_files/cqm\\_amc\\_help.php](http://192.168.145.128/openemr/Documentation/help_files/cqm_amc_help.php)

Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/openemr/; SameSite=Strict

- [http://192.168.145.128/openemr/Documentation/help\\_files/fee\\_sheet\\_help.php](http://192.168.145.128/openemr/Documentation/help_files/fee_sheet_help.php)

Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/openemr/; SameSite=Strict

- [http://192.168.145.128/openemr/Documentation/help\\_files/procedure\\_provider\\_help.php](http://192.168.145.128/openemr/Documentation/help_files/procedure_provider_help.php)

Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/openemr/; SameSite=Strict

- [http://192.168.145.128/openemr/library/dicom\\_frame.php](http://192.168.145.128/openemr/library/dicom_frame.php)

Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/openemr/; SameSite=Strict

- [http://192.168.145.128/openemr/Documentation/help\\_files/report\\_dashboard\\_help.php](http://192.168.145.128/openemr/Documentation/help_files/report_dashboard_help.php)

```
Set-Cookie: OpenEMR=g3GhfKD5xIsb3Ge5m8KYxf43LFTvIbo%2CVxmCKL9iQGY052L; path=/openemr/; SameSite=Strict
```

## Request

---

```
GET /openemr/interface/login/login.php?site=default HTTP/1.1
Host: 192.168.145.128
Pragma: no-cache
Cache-Control: no-cache
accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
accept-language: en-US
upgrade-insecure-requests: 1
Accept-Encoding: gzip,deflate,br
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0 Safari/537.36
```

## Recommendation

---

If possible, you should set the `HttpOnly` flag for these cookies.

## Content Security Policy (CSP) not implemented

---

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks.

Content Security Policy (CSP) can be implemented by adding a `Content-Security-Policy` header. The value of this header is a string containing the policy directives describing your Content Security Policy. To implement CSP, you should define lists of allowed origins for all of the types of resources that your site utilizes. For example, if you have a simple site that needs to load scripts, stylesheets, and images hosted locally, as well as from the jQuery library from their CDN, the CSP header could look like the following:

```
Content-Security-Policy:
default-src 'self';
script-src 'self' https://code.jquery.com;
```

It was detected that your web application doesn't implement Content Security Policy (CSP) as the CSP header is missing from the response. It's recommended to implement Content Security Policy (CSP) into your web application.

## CWE

CWE-1021

## CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

## CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Changed
Confidentiality	None
Integrity Impact	None
Availability Impact	None

## Impact

CSP can be used to prevent and/or mitigate attacks that involve content/code injection, such as cross-site scripting/XSS attacks, attacks that require embedding a malicious resource, attacks that involve malicious use of iframes, such as clickjacking attacks, and others.

## <http://10.10.236.31/>

Paths without CSP header:

- <http://10.10.236.31/openemr/public/assets/i18next/dist/umd/>
- <http://10.10.236.31/openemr/public/assets/select2/>
- <http://10.10.236.31/openemr/interface/>
- <http://10.10.236.31/openemr/public/themes/>
- <http://10.10.236.31/openemr/public/assets/hotkeys-js/>
- [http://10.10.236.31/openemr/library/ajax/i18n\\_generator.php](http://10.10.236.31/openemr/library/ajax/i18n_generator.php)
- <http://10.10.236.31/openemr/public/assets/knockout/>
- <http://10.10.236.31/openemr/public/assets/select2/dist/js/>
- <http://10.10.236.31/openemr/public/assets/i18next/>
- <http://10.10.236.31/openemr/interface/main/messages/>

- [http://10.10.236.31/openemr/interface/product\\_registration/](http://10.10.236.31/openemr/interface/product_registration/)
- <http://10.10.236.31/openemr/public/assets/knockout/build/output/>
- [http://10.10.236.31/openemr/Documentation/help\\_files/](http://10.10.236.31/openemr/Documentation/help_files/)
- <http://10.10.236.31/openemr/public/assets/jquery/>
- <http://10.10.236.31/openemr/public/assets/select2/dist/>
- <http://10.10.236.31/openemr/library/>
- <http://10.10.236.31/openemr/public/assets/select2/dist/css/>
- <http://10.10.236.31/openemr/public/assets/>
- <http://10.10.236.31/openemr/interface/main/messages/css/>
- <http://10.10.236.31/openemr/interface/main/messages/js/>
- <http://10.10.236.31/openemr/library/js/vendors/validate/>

## Request

---

GET /openemr/public/assets/i18next/dist/umd/ HTTP/1.1  
 Acunetix-Aspect: enabled  
 Acunetix-Aspect-Password: 8595e182db21cbbc10c83c2c4cf193d3  
 Acunetix-Aspect-ScanID: 816589585389164376  
 Acunetix-Aspect-Queries: filelist;packages;aspectalerts;routes  
 Referer: http://10.10.236.31/openemr/public/assets/i18next/dist/umd/  
 Cookie: OpenEMR=Dj68HNoGw-vYWT2k81NHDiqIHhLtRgfoVY0Tqo%2Cj6JeJm5aU  
 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
 Accept-Encoding: gzip,deflate,br  
 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)  
 Chrome/109.0.0.0 Safari/537.36  
 Host: 10.10.236.31  
 Connection: Keep-alive

## <http://192.168.145.128/>

Paths without CSP header:

- <http://192.168.145.128/openemr/public/assets/>
- <http://192.168.145.128/openemr/library/>
- <http://192.168.145.128/openemr/public/assets/hotkeys-js/>

- http://192.168.145.128/openemr/interface/main/tabs/
- http://192.168.145.128/openemr/public/assets/knockout/
- http://192.168.145.128/openemr/interface/
- http://192.168.145.128/openemr/interface/main/main\_screen.php
- http://192.168.145.128/openemr/public/assets/bootstrap/dist/js/
- http://192.168.145.128/openemr/public/assets/moment/min/
- http://192.168.145.128/openemr/interface/main/messages/messages.php
- http://192.168.145.128/openemr/public/assets/jquery/dist/
- http://192.168.145.128/openemr/library/ajax/dated\_reminders\_counter.php
- http://192.168.145.128/openemr/public/assets/select2/
- http://192.168.145.128/openemr/library/js/vendors/
- http://192.168.145.128/openemr/interface/main/calendar/
- http://192.168.145.128/openemr/public/assets/jquery/
- http://192.168.145.128/openemr/Documentation/
- http://192.168.145.128/openemr/Documentation/help\_files/
- http://192.168.145.128/openemr/public/assets/i18next/
- http://192.168.145.128/openemr/library/ajax/i18n\_generator.php
- http://192.168.145.128/openemr/library/ajax/

## Request

---

```
GET /openemr/public/assets/ HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/public/assets/
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
```

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

## Recommendation

---

It's recommended to implement Content Security Policy (CSP) into your web application. Configuring Content Security Policy involves adding the **Content-Security-Policy** HTTP header to a web page and giving it values to control resources the user agent is allowed to load for that page.

## References

---

### [Content Security Policy \(CSP\)](#)

<https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP>

### [Implementing Content Security Policy](#)

<https://hacks.mozilla.org/2016/02/implementing-content-security-policy/>

## Content Security Policy Misconfiguration

---

Acunetix evaluated the scan target's Content Security Policies, checked for misconfigurations and potentially unintended side-effects of otherwise valid configurations, and offers the following suggestions on how to change existing policies for improved security and maximum compatibility.

### CWE

CWE-16

## Impact

---

Consult References for more information.

**http://10.10.236.31/**

Verified

- Missing object-src in CSP Declaration

- First observed on: <http://10.10.236.31/openemr/interface/login/login.php>
- CSP Value: frame-ancestors 'none'
- CSP Source: header
- Summary: Acunetix detected that object-src is missed in CSP declaration. It allows the injection of plugins which can execute JavaScript.
- Impact: N/A
- Remediation: Set object-src to 'none' in CSP declaration: Content-Security-Policy: object-src 'none';

- o **References:**

- N/A

## Request

---

```
GET /openemr/interface/login/login.php?site=default HTTP/1.1
Host: 10.10.236.31
Pragma: no-cache
Cache-Control: no-cache
accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
accept-language: en-US
upgrade-insecure-requests: 1
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
```

## <http://192.168.145.128/>

Verified

- **Missing object-src in CSP Declaration**

- o **First observed on:** <http://192.168.145.128/openemr/interface/login/login.php>
  - o **CSP Value:** frame-ancestors 'none'
  - o **CSP Source:** header
  - o **Summary:** Acunetix detected that object-src is missed in CSP declaration. It allows the injection of plugins which can execute JavaScript.
  - o **Impact:** N/A
  - o **Remediation:** Set object-src to 'none' in CSP declaration: Content-Security-Policy: object-src 'none';
  - o **References:**
  - N/A

## Request

---

```
GET /openemr/interface/login/login.php?site=default HTTP/1.1
Host: 192.168.145.128
Pragma: no-cache
Cache-Control: no-cache
accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
accept-language: en-US
upgrade-insecure-requests: 1
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
```

## Recommendation

See alert details for available remediation advice.

## References

### [Using Content Security Policy \(CSP\) to Secure Web Applications](#)

<https://www.invicti.com/blog/web-security/content-security-policy/>

### [The dangers of incorrect CSP implementations](#)

<https://www.invicti.com/blog/web-security/negative-impact-incorrect-csp-implementations/>

### [Leverage Browser Security Features to Secure Your Website](#)

<https://www.invicti.com/blog/web-security/leverage-browser-security-features-secure-website/>

## Content type is not specified

These page(s) does not set a Content-Type header value. This value informs the browser what kind of data to expect. If this header is missing, the browser may incorrectly handle the data. This could lead to security problems.

### CWE

CWE-16

### CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

### CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Unchanged
Confidentiality	None
Integrity Impact	None
Availability Impact	None

## Impact

None

## <http://10.10.236.31/>

Verified

Pages where the content-type header is not specified:

- <http://10.10.236.31/openemr/composer.lock>
- <http://10.10.236.31/openemr/LICENSE>
- <http://10.10.236.31/openemr/Documentation/README.phpacl>
- <http://10.10.236.31/openemr/Documentation/INSTALL>
- <http://10.10.236.31/openemr/interface/main/calendar/modules/PostCalendar/COPYING>
- <http://10.10.236.31/openemr/interface/main/calendar/modules/PostCalendar/README>
- <http://10.10.236.31/openemr/interface/main/calendar/modules/PostCalendar/pntemplates/default/config/default.conf>
- <http://10.10.236.31/openemr/interface/main/calendar/modules/PostCalendar/pntemplates/default/config/lang.en>
- <http://10.10.236.31/openemr/interface/main/calendar/modules/PostCalendar/pntemplates/default/config/navigation.conf>

## Request

```
GET /openemr/composer.lock HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 8595e182db21cbbc10c83c2c4cf193d3
Acunetix-Aspect-ScanID: 816589585389164376
Acunetix-Aspect-Queries: packages;aspectalerts;routes
Referer: http://10.10.236.31/openemr/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 10.10.236.31
Connection: Keep-alive
```

## <http://192.168.145.128/>

Verified

Pages where the content-type header is not specified:

- <http://192.168.145.128/openemr/composer.lock>
- <http://192.168.145.128/openemr/LICENSE>
- <http://192.168.145.128/openemr/Documentation/INSTALL>
- <http://192.168.145.128/openemr/Documentation/README.phpacl>
- <http://192.168.145.128/openemr/library/api.inc>
- <http://192.168.145.128/openemr/library/auth.inc>
- <http://192.168.145.128/openemr/library/calendar.inc>
- [http://192.168.145.128/openemr/library/direct\\_message\\_check.inc](http://192.168.145.128/openemr/library/direct_message_check.inc)
- <http://192.168.145.128/openemr/library/encounter.inc>
- <http://192.168.145.128/openemr/interface/themes/colors/utilities/batch-payments.scss>

- http://192.168.145.128/openemr/library/forms.inc
- http://192.168.145.128/openemr/library/group.inc
- http://192.168.145.128/openemr/library/lab.inc
- http://192.168.145.128/openemr/library/lists.inc
- http://192.168.145.128/openemr/library/options\_listadd.inc
- http://192.168.145.128/openemr/library/patient.inc
- http://192.168.145.128/openemr/library/pid.inc
- http://192.168.145.128/openemr/library/pnotes.inc
- http://192.168.145.128/openemr/interface/themes/core/patient/demographics.scss
- http://192.168.145.128/openemr/library/registry.inc
- http://192.168.145.128/openemr/library/report.inc

## Request

---

```
GET /openemr/composer.lock HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/
Cookie: OpenEMR=F-6X1PVs1YyH8tuel82CU%2CjzXjI%2C2Xj1wHpg%2CMTJEHOAPWa5
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

## Recommendation

---

Set a Content-Type header value for these page(s).

## Error page web server version disclosure

---

Application errors or warning messages may disclose sensitive information about an application's internal workings to an attacker.

Acunetix found the web server version number and a list of modules enabled on the target server. Consult the 'Attack details' section for more information about the affected page.

### CWE

CWE-200

### CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low

### CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network

Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

## Impact

---

Error messages information about an application's internal workings may be used to escalate attacks.

### <http://10.10.236.31/>

#### Request

---

```
GET /KnNz3PhQmq HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 10.10.236.31
Connection: Keep-alive
```

### <http://192.168.145.128/>

#### Request

---

```
GET /OSEbyESLkq HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

## Recommendation

---

Properly configure the web server not to disclose information about an application's internal workings to the user. Consult the 'Web references' section for more information.

## References

---

## [Custom Error Responses \(Apache HTTP Server\)](#)

<https://httpd.apache.org/docs/current/custom-error.html>

## [server\\_tokens \(Nginx\)](#)

[http://nginx.org/en/docs/http/ngx\\_http\\_core\\_module.html#server\\_tokens](http://nginx.org/en/docs/http/ngx_http_core_module.html#server_tokens)

## [Remove Unwanted HTTP Response Headers \(Microsoft IIS\)](#)

<https://blogs.msdn.microsoft.com/varunm/2013/04/23/remove-unwanted-http-response-headers/>

## Permissions-Policy header not implemented

---

The Permissions-Policy header allows developers to selectively enable and disable use of various browser features and APIs.

### CWE

CWE-1021

### CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

### CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Changed
Confidentiality	None
Integrity Impact	None
Availability Impact	None

## Impact

---

### <http://10.10.236.31/>

Locations without Permissions-Policy header:

- <http://10.10.236.31/openemr/interface/login/login.php>
- <http://10.10.236.31/openemr/public/assets/i18next/dist/umd/>
- <http://10.10.236.31/openemr/public/assets/select2/>
- <http://10.10.236.31/openemr/interface/>
- <http://10.10.236.31/openemr/public/themes/>
- <http://10.10.236.31/openemr/public/assets/hotkeys-js/>
- [http://10.10.236.31/openemr/library/ajax/i18n\\_generator.php](http://10.10.236.31/openemr/library/ajax/i18n_generator.php)
- <http://10.10.236.31/openemr/public/assets/select2/dist/js/>

- http://10.10.236.31/openemr/public/assets/knockout/
- http://10.10.236.31/openemr/public/assets/i18next/
- http://10.10.236.31/openemr/interface/main/messages/
- http://10.10.236.31/openemr/interface/product\_registration/
- http://10.10.236.31/openemr/public/assets/knockout/build/output/
- http://10.10.236.31/openemr/Documentation/help\_files/
- http://10.10.236.31/openemr/public/assets/jquery/
- http://10.10.236.31/openemr/public/assets/select2/dist/
- http://10.10.236.31/openemr/library/
- http://10.10.236.31/openemr/public/assets/select2/dist/css/
- http://10.10.236.31/openemr/public/assets/
- http://10.10.236.31/openemr/interface/main/messages/css/
- http://10.10.236.31/openemr/interface/main/messages/js/

## Request

---

```

GET /openemr/interface/login/login.php?site=default HTTP/1.1
Host: 10.10.236.31
Pragma: no-cache
Cache-Control: no-cache
accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
accept-language: en-US
upgrade-insecure-requests: 1
Accept-Encoding: gzip,deflate,br
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36

```

## http://192.168.145.128/

Locations without Permissions-Policy header:

- http://192.168.145.128/openemr/public/assets/
- http://192.168.145.128/openemr/library/
- http://192.168.145.128/openemr/public/assets/hotkeys-js/
- http://192.168.145.128/openemr/interface/main/tabs/
- http://192.168.145.128/openemr/public/assets/knockout/
- http://192.168.145.128/openemr/interface/
- http://192.168.145.128/openemr/interface/main/main\_screen.php
- http://192.168.145.128/openemr/public/assets/bootstrap/dist/js/
- http://192.168.145.128/openemr/public/assets/moment/min/
- http://192.168.145.128/openemr/interface/main/messages/messages.php
- http://192.168.145.128/openemr/public/assets/jquery/dist/
- http://192.168.145.128/openemr/library/ajax/dated\_reminders\_counter.php
- http://192.168.145.128/openemr/interface/main/dated\_reminders/dated\_reminders.php
- http://192.168.145.128/openemr/public/assets/select2/

- <http://192.168.145.128/openemr/library/js/vendors/>
- <http://192.168.145.128/openemr/interface/login/login.php>
- <http://192.168.145.128/openemr/interface/main/calendar/>
- <http://192.168.145.128/openemr/public/assets/jquery/>
- <http://192.168.145.128/openemr/Documentation/>
- [http://192.168.145.128/openemr/Documentation/help\\_files/](http://192.168.145.128/openemr/Documentation/help_files/)
- <http://192.168.145.128/openemr/public/assets/i18next/>

## Request

---

```
GET /openemr/public/assets/ HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/public/assets/
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

## References

---

### [Permissions-Policy / Feature-Policy \(MDN\)](#)

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy>

### [Permissions Policy \(W3C\)](#)

<https://www.w3.org/TR/permissions-policy-1/>

## Subresource Integrity (SRI) not implemented

---

Subresource Integrity (SRI) is a security feature that enables browsers to verify that third-party resources they fetch (for example, from a CDN) are delivered without unexpected manipulation. It works by allowing developers to provide a cryptographic hash that a fetched file must match.

Third-party resources (such as scripts and stylesheets) can be manipulated. An attacker that has access or has hacked the hosting CDN can manipulate or replace the files. SRI allows developers to specify a base64-encoded cryptographic hash of the resource to be loaded. The integrity attribute containing the hash is then added to the <script> HTML element tag. The integrity string consists of a base64-encoded hash, followed by a prefix that depends on the hash algorithm. This prefix can either be sha256, sha384 or sha512.

The script loaded from the external URL specified in the Details section doesn't implement Subresource

Integrity (SRI). It's recommended to implement Subresource Integrity (SRI) for all the scripts loaded from external hosts.

## CWE

CWE-830

## CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

## CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Changed
Confidentiality	None
Integrity Impact	None
Availability Impact	None

## Impact

An attacker that has access or has hacked the hosting CDN can manipulate or replace the files.

## <http://192.168.145.128/openemr/public/assets/checklist-model/>

Pages where SRI is not implemented:

- http://192.168.145.128/openemr/public/assets/checklist-model/  
Script SRC: <https://cdnjs.cloudflare.com/ajax/libs/angular.js/1.4.8/angular.js>
- http://192.168.145.128/openemr/public/assets/checklist-model/  
Script SRC: [https://cdn.rawgit.com/google/code-prettify/master/loader/run\\_prettify.js](https://cdn.rawgit.com/google/code-prettify/master/loader/run_prettify.js)

## Request

```
GET /openemr/public/assets/checklist-model/ HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/public/assets/
Cookie: OpenEMR=g3GhfkD5xIsb3Ge5m8KYxfe43LFtvIbo%2CVxmCKL9iQGY052L
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
```

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)  
Chrome/109.0.0.0 Safari/537.36  
Host: 192.168.145.128  
Connection: Keep-alive

## Recommendation

Use the SRI Hash Generator link (from the References section) to generate a <script> element that implements Subresource Integrity (SRI).

For example, you can use the following <script> element to tell a browser that before executing the https://example.com/example-framework.js script, the browser must first compare the script to the expected hash, and verify that there's a match.

```
<script src="https://example.com/example-framework.js"  
integrity="sha384-oqVuAfXRKap7fdgCY5uykM6+R9GqQ8K/uxy9rx7HNQlGYl1kPzQholwx4JwY8wC"  
crossorigin="anonymous"></script>
```

## References

### Subresource Integrity

[https://developer.mozilla.org/en-US/docs/Web/Security/Subresource\\_Integrity](https://developer.mozilla.org/en-US/docs/Web/Security/Subresource_Integrity)

### SRI Hash Generator

<https://www.srihash.org/>

## No HTTP Redirection

It was detected that your web application uses HTTP protocol, but doesn't automatically redirect users to HTTPS.

### CWE

CWE-16

### CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

### CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Changed
Confidentiality	None

Integrity Impact	None
Availability Impact	None

## Impact

---

In some circumstances, it could be used for a man-in-the-middle (MitM) attack

### <http://10.10.236.31/>

#### Request

---

```
GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 10.10.236.31
Connection: Keep-alive
```

### <http://192.168.145.128/>

#### Request

---

```
GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

## Recommendation

---

It's recommended to implement best practices of HTTP Redirection into your web application. Consult web references for more information

## References

---

### [HTTP Redirections](#)

[https://infosec.mozilla.org/guidelines/web\\_security#http-redirections](https://infosec.mozilla.org/guidelines/web_security#http-redirections)

## CM-7 LEAST FUNCTIONALITY

---

The organization configures the information system to provide only essential capabilities.

No alerts in this category

## IA-2 USER IDENTIFICATION AND AUTHENTICATION

---

The information system uniquely identifies and authenticates users (or processes acting on behalf of users).

No alerts in this category

## MA-2 CONTROLLED MAINTENANCE

---

The organization schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements

### Vulnerable package dependencies [high]

---

One or more packages that are used in your web application are affected by known vulnerabilities. Please consult the details section for more information about each affected package.

CWE

CWE-1104

### Impact

---

The impact of this vulnerability is different for each vulnerable package. It's recommended to investigate each vulnerable package individually.

<http://10.10.236.31/openemr/>

List of vulnerable composer packages:

**Package:** dompdf/dompdf

**Version:** 1.2.2

**CVE:** CVE-2022-41343

**Title:** Files or Directories Accessible to External Parties

**Description:** registerFont in FontMetrics.php in Dompdf before 2.0.1 allows remote file inclusion because a URI validation failure does not halt font registration, as demonstrated by a @font-face rule.

**CVSS V2:**

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

**CWE:** CWE-552

**References:**

- <https://github.com/dompdf/dompdf/releases/tag/v2.0.1>
- <https://github.com/dompdf/dompdf/issues/2994>
- <https://github.com/dompdf/dompdf/pull/2995>
- <https://tantosec.com/blog/cve-2022-41343/>

**Package:** dompdf/dompdf

**Version:** 1.2.2

**CVE:** CVE-2023-23924

**Title:** Incorrect Authorization

**Description:** Dompdf is an HTML to PDF converter. The URI validation on dompdf 2.0.1 can be bypassed on SVG parsing by passing `<image>` tags with uppercase letters. This may lead to arbitrary object unserialize on PHP < 8, through the `phar` URL wrapper. An attacker can exploit the vulnerability to call arbitrary URL with arbitrary protocols, if they can provide a SVG file to dompdf. In PHP versions before 8.0.0, it leads to arbitrary unserialize, that will lead to the very least to an arbitrary file deletion and even remote code execution, depending on classes that are available.

**CVSS V2:**

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

**CWE:** CWE-863

**References:**

- <https://github.com/dompdf/dompdf/security/advisories/GHSA-3cw5-7cxw-v5qg>
- <https://github.com/dompdf/dompdf/releases/tag/v2.0.2>
- <https://github.com/dompdf/dompdf/commit/7558f07f693b2ac3266089f21051e6b78c6a0c85>

**Package:** dompdf/dompdf

**Version:** 1.2.2

**CVE:** CVE-2023-24813

**Title:** Interpretation Conflict

**Description:** Dompdf is an HTML to PDF converter written in php. Due to the difference in the attribute parser of Dompdf and php-svg-lib, an attacker can still call arbitrary URLs with arbitrary protocols. Dompdf parses the href attribute of `image` tags and respects `xlink:href` even if `href` is specified. However, php-svg-lib, which is later used to parse the svg file, parses the href attribute. Since `href` is respected if both `xlink:href` and `href` is specified, it's possible to bypass the protection on the Dompdf side by providing an empty `xlink:href` attribute. An attacker can exploit the vulnerability to call arbitrary URLs with arbitrary protocols if they provide an SVG file to the Dompdf. In PHP versions before 8.0.0, it leads to arbitrary unserialize, which will lead, at the very least, to arbitrary file deletion and might lead to remote code execution, depending on available classes. This vulnerability has been addressed in commit `95009ea98` which has been included in release version 2.0.3. Users are advised to upgrade. There are no known workarounds for this vulnerability.

**CVSS V2:**

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

**CWE:** CWE-436

**References:**

- <https://github.com/dompdf/dompdf/security/advisories/GHSA-56gj-mvh6-rp75>
- <https://github.com/dompdf/dompdf/commit/95009ea98230f9b084b040c34e3869ef3dccc9aa>

**Package:** guzzlehttp/guzzle

**Version:** 7.4.4

**CVE:** CVE-2022-31091

**Title:**

**Description:** Guzzle, an extensible PHP HTTP client. `Authorization` and `Cookie` headers on requests are sensitive information. In affected versions on making a request which responds with a redirect to a URI with a different port, if we choose to follow it, we should remove the `Authorization` and `Cookie` headers from the request, before continuing. Previously, we would only consider a change in host or scheme. Affected Guzzle 7 users should upgrade to Guzzle 7.4.5 as soon as possible. Affected users using any earlier series of Guzzle should upgrade to Guzzle 6.5.8 or 7.4.5. Note that a partial fix was implemented in Guzzle 7.4.2, where a change in host would trigger removal of the curl-added Authorization header, however this earlier fix did not cover change in scheme or change in port. An alternative approach would be to use your own redirect middleware, rather than ours, if you are unable to upgrade. If you do not require or expect redirects to be followed, one should simply disable redirects all together.

**CVSS V2:** AV:N/AC:L/Au:S/C:P/I:N/A:N

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N

**CWE:** NVD-CWE-noinfo

**References:**

- <https://github.com/guzzle/guzzle/commit/1dd98b0564cb3f6bd16ce683cb755f94c10fdb82>
- <https://github.com/guzzle/guzzle/security/advisories/GHSA-q559-8m2m-g699>
- <https://www.debian.org/security/2022/dsa-5246>

**Package:** guzzlehttp/guzzle

**Version:** 7.4.4

**CVE:** CVE-2022-31090

**Title:** Exposure of Sensitive Information to an Unauthorized Actor

**Description:** Guzzle, an extensible PHP HTTP client. `Authorization` headers on requests are sensitive information. In affected versions when using our Curl handler, it is possible to use the `CURLOPT\_HTTPAUTH` option to specify an `Authorization` header. On making a request which responds with a redirect to a URI with a different origin (change in host, scheme or port), if we choose to follow it, we should remove the `CURLOPT\_HTTPAUTH` option before continuing, stopping curl from appending the `Authorization` header to the new request. Affected Guzzle 7 users should upgrade to Guzzle 7.4.5 as soon as possible. Affected users using any earlier series of Guzzle should upgrade to Guzzle 6.5.8 or 7.4.5. Note that a partial fix was implemented in Guzzle 7.4.2, where a change in host would trigger removal of the curl-added Authorization header, however this earlier fix did not cover change in scheme or change in port. If you do not require or expect redirects to be followed, one should simply disable redirects all together. Alternatively, one can specify to use the Guzzle steam handler backend, rather than curl.

**CVSS V2:** AV:N/AC:L/Au:S/C:P/I:N/A:N

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N

**CWE:** CWE-200

**References:**

- <https://github.com/guzzle/guzzle/commit/1dd98b0564cb3f6bd16ce683cb755f94c10fdb82>
- <https://github.com/guzzle/guzzle/security/advisories/GHSA-25mq-v84q-4j7r>

- <https://www.debian.org/security/2022/dsa-5246>

**Package:** knplabs/knp-snappy

**Version:** 1.4.1

**CVE:** CVE-2023-28115

**Title:** Deserialization of Untrusted Data

**Description:** Snappy is a PHP library allowing thumbnail, snapshot or PDF generation from a url or a html page. Prior to version 1.4.2, Snappy is vulnerable to PHAR deserialization due to a lack of checking on the protocol before passing it into the `file\_exists()` function. If an attacker can upload files of any type to the server he can pass in the phar:// protocol to unserialize the uploaded file and instantiate arbitrary PHP objects. This can lead to remote code execution especially when snappy is used with frameworks with documented POP chains like Laravel/Symfony vulnerable developer code. If a user can control the output file from the `generateFromHtml()` function, it will invoke deserialization. This vulnerability is capable of remote code execution if Snappy is used with frameworks or developer code with vulnerable POP chains. It has been fixed in version 1.4.2.

**CVSS V2:**

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

**CWE:** CWE-502

**References:**

- <https://github.com/KnpLabs/snappy/releases/tag/v1.4.2>
- <https://github.com/KnpLabs/snappy/security/advisories/GHSA-gq6w-q6wh-jggc>
- <https://github.com/KnpLabs/snappy/commit/b66f79334421c26d9c244427963fa2d92980b5d3>
- <https://github.com/KnpLabs/snappy/commit/1ee6360cbdbea5d09705909a150df7963a88efd6>
- <https://github.com/KnpLabs/snappy/blob/5126fb5b335ec929a226314d40cd8dad497c3d67/src/Knp/Snappy/AbstractGenerator.php#L670>
- <https://github.com/KnpLabs/snappy/pull/469>

**Package:** phpseclib/phpseclib

**Version:** 2.0.37

**CVE:** CVE-2023-27560

**Title:** Loop with Unreachable Exit Condition ('Infinite Loop')

**Description:** Math/PrimeField.php in phpseclib 3.x before 3.0.19 has an infinite loop with composite primefields.

**CVSS V2:**

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

**CWE:** CWE-835

**References:**

- <https://github.com/phpseclib/phpseclib/commit/6298d1cd55c3ffa44533bd41906caec246b60440>
- <https://github.com/phpseclib/phpseclib/releases/tag/3.0.19>

**Package:** smarty/smarty

**Version:** 2.6.33

**CVE:** CVE-2021-26119

**Title:**

**Description:** Smarty before 3.1.39 allows a Sandbox Escape because \$smarty.template\_object can be accessed in sandbox mode.

**CVSS V2:** AV:N/AC:L/Au:N/C:N/I:P/A:N

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

**CWE:** NVD-CWE-noinfo

**References:**

- <https://github.com/smarty-php/smarty/blob/master/CHANGELOG.md>
- <https://lists.debian.org/debian-lts-announce/2021/04/msg00004.html>
- <https://lists.debian.org/debian-lts-announce/2021/04/msg00014.html>
- <https://security.gentoo.org/glsa/202105-06>
- <https://www.debian.org/security/2022/dsa-5151>

**Package:** smarty/smarty

**Version:** 2.6.33

**CVE:** CVE-2021-26120

**Title:** Improper Control of Generation of Code ('Code Injection')

**Description:** Smarty before 3.1.39 allows code injection via an unexpected function name after a {function name= substring.

**CVSS V2:** AV:N/AC:L/Au:N/C:P/I:P/A:P

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

**CWE:** CWE-94

**References:**

- <https://github.com/smarty-php/smarty/blob/master/CHANGELOG.md>
- <https://lists.debian.org/debian-lts-announce/2021/04/msg00004.html>
- <https://lists.debian.org/debian-lts-announce/2021/04/msg00014.html>
- <https://security.gentoo.org/glsa/202105-06>
- <https://www.debian.org/security/2022/dsa-5151>

**Package:** smarty/smarty

**Version:** 2.6.33

**CVE:** CVE-2017-1000480

**Title:** Improper Control of Generation of Code ('Code Injection')

**Description:** Smarty 3 before 3.1.32 is vulnerable to a PHP code injection when calling fetch() or display() functions on custom resources that does not sanitize template name.

**CVSS V2:** AV:N/AC:L/Au:N/C:P/I:P/A:P

**CVSS V3:** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

**CWE:** CWE-94

**References:**

- [https://github.com/smarty-php/smarty/blob/master/change\\_log.txt](https://github.com/smarty-php/smarty/blob/master/change_log.txt)
- <https://www.debian.org/security/2018/dsa-4094>
- <https://lists.debian.org/debian-lts-announce/2018/02/msg00000.html>
- <https://lists.debian.org/debian-lts-announce/2018/01/msg00023.html>

**Package:** smarty/smarty

**Version:** 2.6.33

**CVE:** CVE-2018-13982

**Title:** Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

**Description:** Smarty\_Security::isTrustedResourceDir() in Smarty before 3.1.33 is prone to a path traversal vulnerability due to insufficient template code sanitization. This allows attackers controlling the executed template code to bypass the trusted directory security restriction and read arbitrary files.

**CVSS V2:** AV:N/AC:L/Au:N/C:P/I:N/A:N

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

**CWE:** CWE-22

**References:**

- <https://github.com/smarty-php/smarty/commit/f9ca3c63d1250bb56b2bda609dcc9dd81f0065f8>
- <https://github.com/smarty-php/smarty/commit/c9dbe1d08c081912d02bd851d1d1b6388f6133d1>
- <https://github.com/smarty-php/smarty/commit/bcedfd6b58bed4a7366336979ebaa5a240581531>
- <https://github.com/smarty-php/smarty/commit/8d21f38dc35c4cd6b31c2f23fc9b8e5adbc56fe>
- <https://github.com/smarty-php/smarty/commit/2e081a51b1effddb23f87952959139ac62654d50>
- [https://github.com/sbaresearch/advisories/tree/public/2018/SBA-ADV-20180420-01\\_Smarty\\_Path\\_Traversal](https://github.com/sbaresearch/advisories/tree/public/2018/SBA-ADV-20180420-01_Smarty_Path_Traversal)
- <https://lists.debian.org/debian-lts-announce/2021/04/msg00004.html>
- <https://lists.debian.org/debian-lts-announce/2021/04/msg00014.html>
- <https://lists.debian.org/debian-lts-announce/2021/10/msg00015.html>

**Package:** smarty/smarty

**Version:** 2.6.33

**CVE:** CVE-2021-21408

**Title:** Improper Input Validation

**Description:** Smarty is a template engine for PHP, facilitating the separation of presentation (HTML/CSS) from application logic. Prior to versions 3.1.43 and 4.0.3, template authors could run restricted static php methods. Users should upgrade to version 3.1.43 or 4.0.3 to receive a patch.

**CVSS V2:** AV:N/AC:L/Au:S/C:P/I:P/A:P

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

**CWE:** CWE-20

**References:**

- <https://github.com/smarty-php/smarty/commit/19ae410bf56007a5ef24441cdc6414619cfaf664>
- <https://github.com/smarty-php/smarty/releases/tag/v3.1.43>
- <https://github.com/smarty-php/smarty/security/advisories/GHSA-4h9c-v5vg-5m6m>
- <https://github.com/smarty-php/smarty/releases/tag/v4.0.3>
- <https://lists.debian.org/debian-lts-announce/2022/05/msg00005.html>
- <https://www.debian.org/security/2022/dsa-5151>
- <https://security.gentoo.org/glsa/202209-09>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/L777JIBIWJV34HS7LXPIDWASG7TT4LNI/>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/BRAJVDRGCIY5UZ2PQHKDTT7RMKG6WJQQ/>

**Package:** smarty/smarty

**Version:** 2.6.33

**CVE:** CVE-2021-29454

**Title:** Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')

**Description:** Smarty is a template engine for PHP, facilitating the separation of presentation (HTML/CSS) from application logic. Prior to versions 3.1.42 and 4.0.2, template authors could run arbitrary PHP code by crafting a malicious math string. If a math string was passed through as user provided data to the math function, external users could run arbitrary PHP code by crafting a malicious math string. Users should upgrade to version 3.1.42 or 4.0.2 to receive a patch.

**CVSS V2:** AV:N/AC:L/Au:S/C:P/I:P/A:P

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

**CWE:** CWE-74

**References:**

- <https://github.com/smarty-php/smarty/commit/215d81a9fa3cd63d82fb3ab56ecaf97cf1e7db71>
- <https://github.com/smarty-php/smarty/security/advisories/GHSA-29gp-2c3m-3j6m>
- <https://packagist.org/packages/smarty/smarty>
- <https://github.com/smarty-php/smarty/releases/tag/v3.1.42>
- <https://www.smarty.net/docs/en/language.function.math.tpl>
- <https://github.com/smarty-php/smarty/releases/tag/v4.0.2>
- <https://lists.debian.org/debian-lts-announce/2022/05/msg00005.html>
- <https://www.debian.org/security/2022/dsa-5151>
- <https://security.gentoo.org/glsa/202209-09>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/L777JIBIWJV34HS7LXPIDWASG7TT4LNI/>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/BRAJVDRGCIY5UZ2PQHKDTT7RMKG6WJQQ/>

**Package:** smarty/smarty

**Version:** 2.6.33

**CVE:** CVE-2022-29221

**Title:** Improper Control of Generation of Code ('Code Injection')

**Description:** Smarty is a template engine for PHP, facilitating the separation of presentation (HTML/CSS) from application logic. Prior to versions 3.1.45 and 4.1.1, template authors could inject php code by choosing a malicious {block} name or {include} file name. Sites that cannot fully trust template authors should upgrade to versions 3.1.45 or 4.1.1 to receive a patch for this issue. There are currently no known workarounds.

**CVSS V2:** AV:N/AC:L/Au:S/C:P/I:P/A:P

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

**CWE:** CWE-94

**References:**

- <https://github.com/smarty-php/smarty/releases/tag/v3.1.45>
- <https://github.com/smarty-php/smarty/security/advisories/GHSA-634x-pc3q-cf4c>
- <https://github.com/smarty-php/smarty/commit/64ad6442ca1da31cefdb5c9874262b702ccddd>
- <https://github.com/smarty-php/smarty/releases/tag/v4.1.1>
- <https://www.debian.org/security/2022/dsa-5151>
- <https://lists.debian.org/debian-lts-announce/2022/05/msg00044.html>
- <https://security.gentoo.org/glsa/202209-09>

- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/L777JIBIWJV34HS7LXPIDWASG7TT4LNI/>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/BRAJVDRGCIY5UZ2PQHKDTT7RMKG6WJQQ/>

**Package:** twig/twig

**Version:** 3.4.1

**CVE:** CVE-2022-39261

**Title:** Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

**Description:** Twig is a template language for PHP. Versions 1.x prior to 1.44.7, 2.x prior to 2.15.3, and 3.x prior to 3.4.3 encounter an issue when the filesystem loader loads templates for which the name is a user input. It is possible to use the `source` or `include` statement to read arbitrary files from outside the templates' directory when using a namespace like `@somewhere/..//some.file`. In such a case, validation is bypassed. Versions 1.44.7, 2.15.3, and 3.4.3 contain a fix for validation of such template names. There are no known workarounds aside from upgrading.

**CVSS V2:**

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

**CWE:** CWE-22

**References:**

- <https://github.com/twigphp/Twig/commit/35f3035c5deb0041da7b84daf02dea074ddc7a0b>
- <https://github.com/twigphp/Twig/security/advisories/GHSA-52m2-vc4m-jj33>
- <https://www.drupal.org/sa-core-2022-016>
- <https://www.debian.org/security/2022/dsa-5248>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/2OKRUHPVLIQVFPPJ2UWC3WV3WQO763NR/>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/AUVTXMNPSZAHS3DWZEM56V5W4NPVR6L7/>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/NWRFPZSR74SYVJKBTKTMYUK36IJ3SQJP/>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/YU4ZYX62H2NUAKKGUES4RZIM4KMTKZ7F/>
- <https://lists.debian.org/debian-lts-announce/2022/10/msg00016.html>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/TW53TFJ6WWNXMUHOFACKATJTS7NIHVQE/>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/WV5TNNJLGG536TJH6DLCIAAZZIPV2GUD/>

## <http://192.168.145.128/openemr/>

List of vulnerable **composer** packages:

**Package:** dompdf/dompdf

**Version:** 1.2.2

**CVE:** CVE-2022-41343

**Title:** Files or Directories Accessible to External Parties

**Description:** registerFont in FontMetrics.php in Dompdf before 2.0.1 allows remote file inclusion because a URI validation failure does not halt font registration, as demonstrated by a @font-face rule.

**CVSS V2:**

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

**CWE:** CWE-552

**References:**

- <https://github.com/dompdf/dompdf/releases/tag/v2.0.1>
- <https://github.com/dompdf/dompdf/issues/2994>
- <https://github.com/dompdf/dompdf/pull/2995>
- <https://tantosec.com/blog/cve-2022-41343/>

**Package:** dompdf/dompdf

**Version:** 1.2.2

**CVE:** CVE-2023-23924

**Title:** Incorrect Authorization

**Description:** Dompdf is an HTML to PDF converter. The URI validation on dompdf 2.0.1 can be bypassed on SVG parsing by passing `<image>` tags with uppercase letters. This may lead to arbitrary object unserialize on PHP < 8, through the `phar` URL wrapper. An attacker can exploit the vulnerability to call arbitrary URL with arbitrary protocols, if they can provide a SVG file to dompdf. In PHP versions before 8.0.0, it leads to arbitrary unserialize, that will lead to the very least to an arbitrary file deletion and even remote code execution, depending on classes that are available.

**CVSS V2:**

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

**CWE:** CWE-863

**References:**

- <https://github.com/dompdf/dompdf/security/advisories/GHSA-3cw5-7cxw-v5qg>
- <https://github.com/dompdf/dompdf/releases/tag/v2.0.2>
- <https://github.com/dompdf/dompdf/commit/7558f07f693b2ac3266089f21051e6b78c6a0c85>

**Package:** dompdf/dompdf

**Version:** 1.2.2

**CVE:** CVE-2023-24813

**Title:** Interpretation Conflict

**Description:** Dompdf is an HTML to PDF converter written in php. Due to the difference in the attribute parser of Dompdf and php-svg-lib, an attacker can still call arbitrary URLs with arbitrary protocols. Dompdf parses the href attribute of `image` tags and respects `xlink:href` even if `href` is specified. However, php-svg-lib, which is later used to parse the svg file, parses the href attribute. Since `href` is respected if both `xlink:href` and `href` is specified, it's possible to bypass the protection on the Dompdf side by providing an empty `xlink:href` attribute. An attacker can exploit the vulnerability to call arbitrary URLs with arbitrary protocols if they provide an SVG file to the Dompdf. In PHP versions before 8.0.0, it leads to arbitrary unserialize, which will lead, at the very least, to arbitrary file deletion and might lead to remote code execution, depending on available classes. This vulnerability has been addressed in commit `95009ea98` which has been included in release version 2.0.3. Users are advised to upgrade. There are no known workarounds for this vulnerability.

**CVSS V2:**

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

**CWE:** CWE-436

**References:**

- <https://github.com/dompdf/dompdf/security/advisories/GHSA-56gj-mvh6-rp75>
- <https://github.com/dompdf/dompdf/commit/95009ea98230f9b084b040c34e3869ef3dccc9aa>

**Package:** guzzlehttp/guzzle

**Version:** 7.4.4

**CVE:** CVE-2022-31091

**Title:**

**Description:** Guzzle, an extensible PHP HTTP client. `Authorization` and `Cookie` headers on requests are sensitive information. In affected versions on making a request which responds with a redirect to a URI with a different port, if we choose to follow it, we should remove the `Authorization` and `Cookie` headers from the request, before containing. Previously, we would only consider a change in host or scheme. Affected Guzzle 7 users should upgrade to Guzzle 7.4.5 as soon as possible. Affected users using any earlier series of Guzzle should upgrade to Guzzle 6.5.8 or 7.4.5. Note that a partial fix was implemented in Guzzle 7.4.2, where a change in host would trigger removal of the curl-added Authorization header, however this earlier fix did not cover change in scheme or change in port. An alternative approach would be to use your own redirect middleware, rather than ours, if you are unable to upgrade. If you do not require or expect redirects to be followed, one should simply disable redirects all together.

**CVSS V2:** AV:N/AC:L/Au:S/C:P/I:N/A:N

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

**CWE:** NVD-CWE-noinfo

**References:**

- <https://github.com/guzzle/guzzle/commit/1dd98b0564cb3f6bd16ce683cb755f94c10fdbd82>
- <https://github.com/guzzle/guzzle/security/advisories/GHSA-q559-8m2m-g699>
- <https://www.debian.org/security/2022/dsa-5246>

**Package:** guzzlehttp/guzzle

**Version:** 7.4.4

**CVE:** CVE-2022-31090

**Title:** Exposure of Sensitive Information to an Unauthorized Actor

**Description:** Guzzle, an extensible PHP HTTP client. `Authorization` headers on requests are sensitive information. In affected versions when using our Curl handler, it is possible to use the `CURLOPT\_HTTPAUTH` option to specify an `Authorization` header. On making a request which responds with a redirect to a URI with a different origin (change in host, scheme or port), if we choose to follow it, we should remove the `CURLOPT\_HTTPAUTH` option before continuing, stopping curl from appending the `Authorization` header to the new request. Affected Guzzle 7 users should upgrade to Guzzle 7.4.5 as soon as possible. Affected users using any earlier series of Guzzle should upgrade to Guzzle 6.5.8 or 7.4.5. Note that a partial fix was implemented in Guzzle 7.4.2, where a change in host would trigger removal of the curl-added Authorization header, however this earlier fix did not cover change in scheme or change in port. If you do not require or expect redirects to be followed, one should simply disable redirects all together. Alternatively, one can specify to use the Guzzle steam handler backend, rather than curl.

**CVSS V2:** AV:N/AC:L/Au:S/C:P/I:N/A:N

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

**CWE:** CWE-200

**References:**

- <https://github.com/guzzle/guzzle/commit/1dd98b0564cb3f6bd16ce683cb755f94c10fdb82>
- <https://github.com/guzzle/guzzle/security/advisories/GHSA-25mq-v84q-4j7r>
- <https://www.debian.org/security/2022/dsa-5246>

**Package:** knplabs/knp-snappy

**Version:** 1.4.1

**CVE:** CVE-2023-28115

**Title:** Deserialization of Untrusted Data

**Description:** Snappy is a PHP library allowing thumbnail, snapshot or PDF generation from a url or a html page. Prior to version 1.4.2, Snappy is vulnerable to PHAR deserialization due to a lack of checking on the protocol before passing it into the `file\_exists()` function. If an attacker can upload files of any type to the server he can pass in the phar:// protocol to unserialize the uploaded file and instantiate arbitrary PHP objects. This can lead to remote code execution especially when snappy is used with frameworks with documented POP chains like Laravel/Symfony vulnerable developer code. If a user can control the output file from the `generateFromHtml()` function, it will invoke deserialization. This vulnerability is capable of remote code execution if Snappy is used with frameworks or developer code with vulnerable POP chains. It has been fixed in version 1.4.2.

**CVSS V2:**

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

**CWE:** CWE-502

**References:**

- <https://github.com/KnpLabs/snappy/releases/tag/v1.4.2>
- <https://github.com/KnpLabs/snappy/security/advisories/GHSA-gq6w-q6wh-jggc>
- <https://github.com/KnpLabs/snappy/commit/b66f79334421c26d9c244427963fa2d92980b5d3>
- <https://github.com/KnpLabs/snappy/commit/1ee6360cbdbea5d09705909a150df7963a88efd6>
- <https://github.com/KnpLabs/snappy/blob/5126fb5b335ec929a226314d40cd8dad497c3d67/src/Knp/Snappy/AbstractGenerator.php#L670>

- <https://github.com/KnpLabs/snappy/pull/469>

**Package:** phpseclib/phpseclib

**Version:** 2.0.37

**CVE:** CVE-2023-27560

**Title:** Loop with Unreachable Exit Condition ('Infinite Loop')

**Description:** Math/PrimeField.php in phpseclib 3.x before 3.0.19 has an infinite loop with composite primefields.

**CVSS V2:**

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

**CWE:** CWE-835

**References:**

- <https://github.com/phpseclib/phpseclib/commit/6298d1cd55c3ffa44533bd41906caec246b60440>
- <https://github.com/phpseclib/phpseclib/releases/tag/3.0.19>

**Package:** smarty/smarty

**Version:** 2.6.33

**CVE:** CVE-2021-26119

**Title:**

**Description:** Smarty before 3.1.39 allows a Sandbox Escape because \$smarty.template\_object can be accessed in sandbox mode.

**CVSS V2:** AV:N/AC:L/Au:N/C:N/I:P/A:N

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

**CWE:** NVD-CWE-noinfo

**References:**

- <https://github.com/smarty-php/smarty/blob/master/CHANGELOG.md>
- <https://lists.debian.org/debian-lts-announce/2021/04/msg00004.html>
- <https://lists.debian.org/debian-lts-announce/2021/04/msg00014.html>
- <https://security.gentoo.org/glsa/202105-06>
- <https://www.debian.org/security/2022/dsa-5151>

**Package:** smarty/smarty

**Version:** 2.6.33

**CVE:** CVE-2021-26120

**Title:** Improper Control of Generation of Code ('Code Injection')

**Description:** Smarty before 3.1.39 allows code injection via an unexpected function name after a {function name= substring.

**CVSS V2:** AV:N/AC:L/Au:N/C:P/I:P/A:P

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

**CWE:** CWE-94

**References:**

- <https://github.com/smarty-php/smarty/blob/master/CHANGELOG.md>
- <https://lists.debian.org/debian-lts-announce/2021/04/msg00004.html>
- <https://lists.debian.org/debian-lts-announce/2021/04/msg00014.html>
- <https://security.gentoo.org/glsa/202105-06>
- <https://www.debian.org/security/2022/dsa-5151>

**Package:** smarty/smarty

**Version:** 2.6.33

**CVE:** CVE-2017-1000480

**Title:** Improper Control of Generation of Code ('Code Injection')

**Description:** Smarty 3 before 3.1.32 is vulnerable to a PHP code injection when calling fetch() or display() functions on custom resources that does not sanitize template name.

**CVSS V2:** AV:N/AC:L/Au:N/C:P/I:P/A:P

**CVSS V3:** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

**CWE:** CWE-94

**References:**

- [https://github.com/smarty-php/smarty/blob/master/change\\_log.txt](https://github.com/smarty-php/smarty/blob/master/change_log.txt)
- <https://www.debian.org/security/2018/dsa-4094>

- <https://lists.debian.org/debian-lts-announce/2018/02/msg00000.html>
- <https://lists.debian.org/debian-lts-announce/2018/01/msg00023.html>

**Package:** smarty/smarty

**Version:** 2.6.33

**CVE:** CVE-2018-13982

**Title:** Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

**Description:** Smarty\_Security::isTrustedResourceDir() in Smarty before 3.1.33 is prone to a path traversal vulnerability due to insufficient template code sanitization. This allows attackers controlling the executed template code to bypass the trusted directory security restriction and read arbitrary files.

**CVSS V2:** AV:N/AC:L/Au:N/C:P/I:N/A:N

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

**CWE:** CWE-22

**References:**

- <https://github.com/smarty-php/smarty/commit/f9ca3c63d1250bb56b2bda609dcc9dd81f0065f8>
- <https://github.com/smarty-php/smarty/commit/c9dbe1d08c081912d02bd851d1d1b6388f6133d1>
- <https://github.com/smarty-php/smarty/commit/bcedfd6b58bed4a7366336979ebaa5a240581531>
- <https://github.com/smarty-php/smarty/commit/8d21f38dc35c4cd6b31c2f23fc9b8e5adbc56dfe>
- <https://github.com/smarty-php/smarty/commit/2e081a51b1effddb23f87952959139ac62654d50>
- [https://github.com/sbaresearch/advisories/tree/public/2018/SBA-ADV-20180420-01\\_Smarty\\_Path\\_Traversal](https://github.com/sbaresearch/advisories/tree/public/2018/SBA-ADV-20180420-01_Smarty_Path_Traversal)
- <https://lists.debian.org/debian-lts-announce/2021/04/msg00004.html>
- <https://lists.debian.org/debian-lts-announce/2021/04/msg00014.html>
- <https://lists.debian.org/debian-lts-announce/2021/10/msg00015.html>

**Package:** smarty/smarty

**Version:** 2.6.33

**CVE:** CVE-2021-21408

**Title:** Improper Input Validation

**Description:** Smarty is a template engine for PHP, facilitating the separation of presentation (HTML/CSS) from application logic. Prior to versions 3.1.43 and 4.0.3, template authors could run restricted static php methods. Users should upgrade to version 3.1.43 or 4.0.3 to receive a patch.

**CVSS V2:** AV:N/AC:L/Au:S/C:P/I:P/A:P

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

**CWE:** CWE-20

**References:**

- <https://github.com/smarty-php/smarty/commit/19ae410bf56007a5ef24441cdc6414619cfaf664>
- <https://github.com/smarty-php/smarty/releases/tag/v3.1.43>
- <https://github.com/smarty-php/smarty/security/advisories/GHSA-4h9c-v5vg-5m6m>
- <https://github.com/smarty-php/smarty/releases/tag/v4.0.3>
- <https://lists.debian.org/debian-lts-announce/2022/05/msg00005.html>
- <https://www.debian.org/security/2022/dsa-5151>
- <https://security.gentoo.org/glsa/202209-09>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/L777JIBIWJV34HS7LXPIDWASG7TT4LNI/>

- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/BRAJVDRGCIY5UZ2PQHKDTT7RMKG6WJQQ/>

**Package:** smarty/smarty

**Version:** 2.6.33

**CVE:** CVE-2021-29454

**Title:** Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')

**Description:** Smarty is a template engine for PHP, facilitating the separation of presentation (HTML/CSS) from application logic. Prior to versions 3.1.42 and 4.0.2, template authors could run arbitrary PHP code by crafting a malicious math string. If a math string was passed through as user provided data to the math function, external users could run arbitrary PHP code by crafting a malicious math string. Users should upgrade to version 3.1.42 or 4.0.2 to receive a patch.

**CVSS V2:** AV:N/AC:L/Au:S/C:P/I:P/A:P

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

**CWE:** CWE-74

**References:**

- <https://github.com/smarty-php/smarty/commit/215d81a9fa3cd63d82fb3ab56ecaf97cf1e7db71>
- <https://github.com/smarty-php/smarty/security/advisories/GHSA-29gp-2c3m-3j6m>
- <https://packagist.org/packages/smarty/smarty>
- <https://github.com/smarty-php/smarty/releases/tag/v3.1.42>
- <https://www.smarty.net/docs/en/language.function.math.tpl>
- <https://github.com/smarty-php/smarty/releases/tag/v4.0.2>
- <https://lists.debian.org/debian-lts-announce/2022/05/msg00005.html>
- <https://www.debian.org/security/2022/dsa-5151>
- <https://security.gentoo.org/glsa/202209-09>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/L777JIBIWJV34HS7LXPIDWASG7TT4LNI/>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/BRAJVDRGCIY5UZ2PQHKDTT7RMKG6WJQQ/>

**Package:** smarty/smarty

**Version:** 2.6.33

**CVE:** CVE-2022-29221

**Title:** Improper Control of Generation of Code ('Code Injection')

**Description:** Smarty is a template engine for PHP, facilitating the separation of presentation (HTML/CSS) from application logic. Prior to versions 3.1.45 and 4.1.1, template authors could inject php code by choosing a malicious {block} name or {include} file name. Sites that cannot fully trust template authors should upgrade to versions 3.1.45 or 4.1.1 to receive a patch for this issue. There are currently no known workarounds.

**CVSS V2:** AV:N/AC:L/Au:S/C:P/I:P/A:P

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

**CWE:** CWE-94

**References:**

- <https://github.com/smarty-php/smarty/releases/tag/v3.1.45>
- <https://github.com/smarty-php/smarty/security/advisories/GHSA-634x-pc3q-cf4c>
- <https://github.com/smarty-php/smarty/commit/64ad6442ca1da31cefdab5c9874262b702ccddd>

- <https://github.com/smarty-php/smarty/releases/tag/v4.1.1>
- <https://www.debian.org/security/2022/dsa-5151>
- <https://lists.debian.org/debian-lts-announce/2022/05/msg00044.html>
- <https://security.gentoo.org/glsa/202209-09>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/L777JIBIWJV34HS7LXPIDWASG7TT4LNI/>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/BRAJVDRGCIY5UZ2PQHKDTT7RMKG6WJQQ/>

**Package:** twig/twig

**Version:** 3.4.1

**CVE:** CVE-2022-39261

**Title:** Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

**Description:** Twig is a template language for PHP. Versions 1.x prior to 1.44.7, 2.x prior to 2.15.3, and 3.x prior to 3.4.3 encounter an issue when the filesystem loader loads templates for which the name is a user input. It is possible to use the `source` or `include` statement to read arbitrary files from outside the templates' directory when using a namespace like `@somewhere/..//some.file`. In such a case, validation is bypassed. Versions 1.44.7, 2.15.3, and 3.4.3 contain a fix for validation of such template names. There are no known workarounds aside from upgrading.

**CVSS V2:**

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

**CWE:** CWE-22

**References:**

- <https://github.com/twigphp/Twig/commit/35f3035c5deb0041da7b84daf02dea074ddc7a0b>
- <https://github.com/twigphp/Twig/security/advisories/GHSA-52m2-vc4m-jj33>
- <https://www.drupal.org/sa-core-2022-016>
- <https://www.debian.org/security/2022/dsa-5248>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/2OKRUHPVLIQVFPPJ2UWC3WV3WQO763NR/>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/AUVTXMNPSZAHS3DWZEM56V5W4NPVR6L7/>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/NWRFPZSR74SYVJKBTKTMYUK36IJ3SQJP/>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/YU4ZYX62H2NUAKKGUES4RZIM4KMTKZ7F/>
- <https://lists.debian.org/debian-lts-announce/2022/10/msg00016.html>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/TW53TFJ6WWNXMUHOFACKATJTS7NIHVQE/>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/WV5TNNJLGG536TJH6DLCIAAZZIPV2GUD/>

## Recommendation

---

It's recommended to update the vulnerable packages to the latest version (if a fix exists). If a fix does not exist, you may want to suggest changes that address the vulnerability to the package maintainer or remove the package from your dependency tree.

## Vulnerable package dependencies [medium]

---

One or more packages that are used in your web application are affected by known vulnerabilities. Please consult the details section for more information about each affected package.

### CWE

CWE-1104

## Impact

---

The impact of this vulnerability is different for each vulnerable package. It's recommended to investigate each vulnerable package individually.

### <http://10.10.236.31/openemr/>

List of vulnerable **composer** packages:

**Package:** dompdf/dompdf

**Version:** 1.2.2

**CVE:** CVE-2022-0085

**Title:** Server-Side Request Forgery (SSRF)

**Description:** Server-Side Request Forgery (SSRF) in GitHub repository dompdf/dompdf prior to 2.0.0.

**CVSS V2:** AV:N/AC:M/Au:N/C:N/I:P/A:N

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

**CWE:** CWE-918

**References:**

- <https://github.com/dompdf/dompdf/commit/bb1ef65011a14730b7cfbe73506b4bb8a03704bd>
- <https://huntr.dev/bounties/73dbcc78-5ba9-492f-9133-13bbc9f31236>

**Package:** dompdf/dompdf

**Version:** 1.2.2

**CVE:** CVE-2022-2400

**Title:** External Control of File Name or Path

**Description:** External Control of File Name or Path in GitHub repository dompdf/dompdf prior to 2.0.0.

**CVSS V2:**

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

**CWE:** CWE-73

**References:**

- <https://huntr.dev/bounties/a6da5e5e-86be-499a-a3c3-2950f749202a>
- <https://github.com/dompdf/dompdf/commit/99aeec1efec9213e87098d42eb09439e7ee0bb6a>

**Package:** smarty/smarty

**Version:** 2.6.33

**CVE:** CVE-2018-16831

**Title:** Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

**Description:** Smarty before 3.1.33-dev-4 allows attackers to bypass the trusted\_dir protection mechanism via a file:../ substring in an include statement.

**CVSS V2:** AV:N/AC:M/Au:N/C:C/I:N/A:N

**CVSS V3:** CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N

**CWE:** CWE-22

**References:**

- <https://github.com/smarty-php/smarty/issues/486>

**Package:** smarty/smarty

**Version:** 2.6.33

**CVE:** CVE-2018-25047

**Title:** Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

**Description:** In Smarty before 3.1.47 and 4.x before 4.2.1, libs/plugins/function.mailto.php allows XSS. A web page that uses smarty\_function\_mailto, and that could be parameterized using GET or POST input parameters, could allow injection of JavaScript code by a user.

**CVSS V2:**

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N

**CWE:** CWE-79

**References:**

- <https://github.com/smarty-php/smarty/releases/tag/v4.2.1>
- <https://github.com/smarty-php/smarty/releases/tag/v3.1.47>
- <https://bugs.gentoo.org/870100>
- <https://github.com/smarty-php/smarty/issues/454>
- <https://security.gentoo.org/glsa/202209-09>
- <https://lists.debian.org/debian-lts-announce/2023/01/msg00002.html>

**Package:** smarty/smarty

**Version:** 2.6.33

**CVE:** CVE-2023-28447

**Title:** Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

**Description:** Smarty is a template engine for PHP. In affected versions smarty did not properly escape javascript code. An attacker could exploit this vulnerability to execute arbitrary JavaScript code in the context of the user's browser session. This may lead to unauthorized access to sensitive user data, manipulation of the web application's behavior, or unauthorized actions performed on behalf of the user. Users are advised to upgrade to either version 3.1.48 or to 4.3.1 to resolve this issue. There are no known workarounds for this vulnerability.

**CVSS V2:**

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

**CWE:** CWE-79

**References:**

- <https://github.com/smarty-php/smarty/security/advisories/GHSA-7j98-h7fp-4vwj>
- <https://github.com/smarty-php/smarty/commit/685662466f653597428966d75a661073104d713d>

## <http://192.168.145.128/openemr/>

List of vulnerable **composer** packages:

**Package:** dompdf/dompdf

**Version:** 1.2.2

**CVE:** CVE-2022-0085

**Title:** Server-Side Request Forgery (SSRF)

**Description:** Server-Side Request Forgery (SSRF) in GitHub repository dompdf/dompdf prior to 2.0.0.

**CVSS V2:** AV:N/AC:M/Au:N/C:N/I:P/A:N

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

**CWE:** CWE-918

**References:**

- <https://github.com/dompdf/dompdf/commit/bb1ef65011a14730b7cfbe73506b4bb8a03704bd>
- <https://huntr.dev/bounties/73dbcc78-5ba9-492f-9133-13bbc9f31236>

**Package:** dompdf/dompdf

**Version:** 1.2.2

**CVE:** CVE-2022-2400

**Title:** External Control of File Name or Path

**Description:** External Control of File Name or Path in GitHub repository dompdf/dompdf prior to 2.0.0.

**CVSS V2:**

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

**CWE:** CWE-73

**References:**

- <https://huntr.dev/bounties/a6da5e5e-86be-499a-a3c3-2950f749202a>
- <https://github.com/dompdf/dompdf/commit/99aec1efec9213e87098d42eb09439e7ee0bb6a>

**Package:** smarty/smarty

**Version:** 2.6.33

**CVE:** CVE-2018-16831

**Title:** Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

**Description:** Smarty before 3.1.33-dev-4 allows attackers to bypass the trusted\_dir protection mechanism via a file:../../ substring in an include statement.

**CVSS V2:** AV:N/AC:M/Au:N/C:C/I:N/A:N

**CVSS V3:** CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N

**CWE:** CWE-22

**References:**

- <https://github.com/smarty-php/smarty/issues/486>

**Package:** smarty/smarty

**Version:** 2.6.33

**CVE:** CVE-2018-25047

**Title:** Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

**Description:** In Smarty before 3.1.47 and 4.x before 4.2.1, libs/plugins/function.mailto.php allows XSS. A web page that uses smarty\_function\_mailto, and that could be parameterized using GET or POST input parameters, could allow injection of JavaScript code by a user.

**CVSS V2:**

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N

**CWE:** CWE-79

**References:**

- <https://github.com/smarty-php/smarty/releases/tag/v4.2.1>
- <https://github.com/smarty-php/smarty/releases/tag/v3.1.47>
- <https://bugs.gentoo.org/870100>
- <https://github.com/smarty-php/smarty/issues/454>
- <https://security.gentoo.org/glsa/202209-09>
- <https://lists.debian.org/debian-lts-announce/2023/01/msg00002.html>

**Package:** smarty/smarty

**Version:** 2.6.33

**CVE:** CVE-2023-28447

**Title:** Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

**Description:** Smarty is a template engine for PHP. In affected versions smarty did not properly escape javascript code. An attacker could exploit this vulnerability to execute arbitrary JavaScript code in the context of the user's browser session. This may lead to unauthorized access to sensitive user data, manipulation of the web application's behavior, or unauthorized actions performed on behalf of the user. Users are advised to upgrade to either version 3.1.48 or to 4.3.1 to resolve this issue. There are no known workarounds for this vulnerability.

**CVSS V2:**

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

**CWE:** CWE-79

**References:**

- <https://github.com/smarty-php/smarty/security/advisories/GHSA-7j98-h7fp-4vwj>
- <https://github.com/smarty-php/smarty/commit/685662466f653597428966d75a661073104d713d>

## Recommendation

It's recommended to update the vulnerable packages to the latest version (if a fix exists). If a fix does not exist, you may want to suggest changes that address the vulnerability to the package maintainer or

remove the package from your dependency tree.

## Vulnerable JavaScript libraries

---

You are using one or more vulnerable JavaScript libraries. One or more vulnerabilities were reported for this version of the library. Consult Attack details and Web References for more information about the affected library and the vulnerabilities that were reported.

### CWE

CWE-937

### CVSS2

AV:N/AC:L/Au:N/C:P/I:P/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	Partial
Availability Impact	None

### CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N

Base Score	6.5
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	Low
Availability Impact	None

## Impact

---

Consult References for more information.

<http://10.10.236.31/>

Confidence: 95%

- **jQuery 1.10.2**
  - URL: <http://10.10.236.31/openemr/public/assets/jquery-datetimepicker/>
  - Detection method: The library's name and version were determined based on its dynamic behavior.
  - CVE-ID: CVE-2015-9251, CVE-2020-11022, CVE-2020-11023
  - Description: Possible Cross Site Scripting via third-party text/javascript responses / In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. / In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing option elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.
  - References:

- <https://github.com/jquery/jquery/issues/2432>
- <http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/>
- <https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/>
- <https://mksben.lo.cm/2020/05/jquery3.5.0-xss.html>
- <https://jquery.com/upgrade-guide/3.5/>
- <https://api.jquery.com/jQuery.htmlPrefilter/>
- <https://www.cvedetails.com/cve/CVE-2020-11022/>
- <https://github.com/advisories/GHSA-gxr4-xjj5-5px2>
- <https://www.cvedetails.com/cve/CVE-2020-11023/>
- <https://github.com/advisories/GHSA-jpcq-cgw6-v4j6>

## Request

---

```
GET /openemr/public/assets/jquery-datetimepicker/ HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 8595e182db21cbbc10c83c2c4cf193d3
Acunetix-Aspect-ScanID: 816589585389164376
Acunetix-Aspect-Queries: filelist;packages;aspectalerts;routes
Referer: http://10.10.236.31/openemr/public/assets/jquery-datetimepicker/
Cookie: OpenEMR=Dj68HNoGw-vYWT2k81NHDiqIHhLtRgfoVY0Tqo%2Cj6JeJm5aU
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 10.10.236.31
Connection: Keep-alive
```

## <http://10.10.236.31/>

Verified

- **jQuery UI 1.12.1**

- URL: <http://10.10.236.31/openemr/public/assets/jquery-ui/jquery-ui.js>
- Detection method: The library's name and version were determined based on the file's syntax fingerprint, and contents. Acunetix verified the library version and the associated vulnerabilities with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- CVE-ID: CVE-2021-41184
- Description: XSS in the 'of' option of the '.position()' util
- References:
  - <https://blog.jqueryui.com/2021/10/jquery-ui-1-13-0-released/>
  - <https://github.com/jquery/jquery-ui/security/advisories/GHSA-gpqq-952q-5327>

## Request

---

```
GET /openemr/public/assets/jquery-ui/jquery-ui.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 8595e182db21cbbc10c83c2c4cf193d3
Acunetix-Aspect-ScanID: 816589585389164376
Acunetix-Aspect-Queries: aspectalerts;routes
```

Referer: http://10.10.236.31/openemr/Documentation/help\_files/openemr\_installation\_help.php  
Cookie: OpenEMR=b3DHM9s5BR72IjC3y6GcpBb736abtMj3%2CfzaSNeoS-j94pMx  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
Accept-Encoding: gzip,deflate,br  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)  
Chrome/109.0.0.0 Safari/537.36  
Host: 10.10.236.31  
Connection: Keep-alive

**http://10.10.236.31/**

Confidence: 95%

- **jQuery UI Datepicker 1.12.1**

- URL: http://10.10.236.31/openemr/public/assets/jquery-ui/jquery-ui.js
- Detection method: The library's name and version were determined based on the file's contents.
- CVE-ID: CVE-2021-41182, CVE-2021-41183
- Description: XSS in the 'altField' option of the Datepicker widget / XSS in '\*Text' options of the Datepicker widget
- References:
  - https://blog.jqueryui.com/2021/10/jquery-ui-1-13-0-released/
  - https://github.com/jquery/jquery-ui/security/advisories/GHSA-9gj3-hwp5-pmwv
  - https://github.com/jquery/jquery-ui/security/advisories/GHSA-j7qv-pgf6-hvh4

## Request

GET /openemr/public/assets/jquery-ui/jquery-ui.js HTTP/1.1  
Acunetix-Aspect: enabled  
Acunetix-Aspect-Password: 8595e182db21cbbc10c83c2c4cf193d3  
Acunetix-Aspect-ScanID: 816589585389164376  
Acunetix-Aspect-Queries: aspectalerts;routes  
Referer: http://10.10.236.31/openemr/Documentation/help\_files/openemr\_installation\_help.php  
Cookie: OpenEMR=b3DHM9s5BR72IjC3y6GcpBb736abtMj3%2CfzaSNeoS-j94pMx  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
Accept-Encoding: gzip,deflate,br  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)  
Chrome/109.0.0.0 Safari/537.36  
Host: 10.10.236.31  
Connection: Keep-alive

**http://10.10.236.31/**

Verified

- **jQuery 1.12.4**

- URL: http://10.10.236.31/openemr/public/assets/jquery-ui/external/jquery/jquery.js
- Detection method: The library's name and version were determined based on the file's syntax fingerprint, and contents. Acunetix verified the library version and the associated vulnerabilities with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.

- CVE-ID: CVE-2015-9251, CVE-2020-11022, CVE-2020-11023
- Description: Possible Cross Site Scripting via third-party text/javascript responses (1.12.0-1.12.2 mitigation reverted) / In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. / In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing option elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.
- References:
  - <https://github.com/jquery/jquery/issues/2432>
  - <https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/>
  - <https://mksben.lo.cm/2020/05/jquery3.5.0-xss.html>
  - <https://jquery.com/upgrade-guide/3.5/>
  - <https://api.jquery.com/jQuery.htmlPrefilter/>
  - <https://www.cvedetails.com/cve/CVE-2020-11022/>
  - <https://github.com/advisories/GHSA-gxr4-xjj5-5px2>
  - <https://www.cvedetails.com/cve/CVE-2020-11023/>
  - <https://github.com/advisories/GHSA-jpcq-cgw6-v4j6>

## Request

---

```
GET /openemr/public/assets/jquery-ui/external/jquery/jquery.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 8595e182db21cbbc10c83c2c4cf193d3
Acunetix-Aspect-ScanID: 816589585389164376
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://10.10.236.31/openemr/public/assets/jquery-ui/
Cookie: OpenEMR=b3DHM9s5BR72IjC3y6GcpBb736abtMj3%2CfzaSNeoS-j94pMx
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 10.10.236.31
Connection: Keep-alive
```

**http://192.168.145.128/**

Confidence: 95%

- AngularJS 1.4.8

- URL: <https://cdnjs.cloudflare.com/ajax/libs/angular.js/1.4.8/angular.js>
- Detection method: The library's name and version were determined based on the file's CDN URI.
- CVE-ID: CVE-2020-7676
- Description: Prototype pollution / Cross-Site Scripting.
- References:
  - <https://github.com/angular/angular.js/commit/726f49dcf6c23106ddaf5cf5e2e592841db743a>
  - <https://github.com/angular/angular.js/blob/master/CHANGELOG.md#179-pollution-eradication-2019-11-19>

- <https://nvd.nist.gov/vuln/detail/CVE-2020-7676>

## Request

---

```
GET /openemr/public/assets/checklist-model/ HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/public/assets/
Cookie: OpenEMR=g3GhfkD5xIsb3Ge5m8KYxfe43LFtvIbo%2CVxmCKL9iQGY052L
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

**http://192.168.145.128/**

Verified

- **jQuery UI 1.12.1**

- URL: <http://192.168.145.128/openemr/public/assets/jquery-ui/jquery-ui.js>
- Detection method: The library's name and version were determined based on the file's syntax fingerprint, and contents. Acunetix verified the library version and the associated vulnerabilities with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- CVE-ID: CVE-2021-41184
- Description: XSS in the 'of' option of the '.position()' util
- References:
  - <https://blog.jqueryui.com/2021/10/jquery-ui-1-13-0-released/>
  - <https://github.com/jquery/jquery-ui/security/advisories/GHSA-gpqq-952q-5327>

## Request

---

```
GET /openemr/public/assets/jquery-ui/jquery-ui.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/Documentation/help_files/openemr_installation_help.php
Cookie: OpenEMR=d40D5DeY1SqGsuSImcMvd1XbnUvSB1Sl%2CNIItqLcdHnpIKp4G
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

<http://192.168.145.128/>

Confidence: 95%

- **jQuery UI Datepicker 1.12.1**

- URL: <http://192.168.145.128/openemr/public/assets/jquery-ui/jquery-ui.js>
- Detection method: The library's name and version were determined based on the file's contents.
- CVE-ID: CVE-2021-41182, CVE-2021-41183
- Description: XSS in the 'altField' option of the Datepicker widget / XSS in '\*Text' options of the Datepicker widget
- References:
  - <https://blog.jqueryui.com/2021/10/jquery-ui-1-13-0-released/>
  - <https://github.com/jquery/jquery-ui/security/advisories/GHSA-9gj3-hwp5-pmw>
  - <https://github.com/jquery/jquery-ui/security/advisories/GHSA-j7qv-pgf6-hvh4>

## Request

---

```
GET /openemr/public/assets/jquery-ui/jquery-ui.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/Documentation/help_files/openemr_installation_help.php
Cookie: OpenEMR=d40D5DeY1SqGsuSImcMvd1XbnUvSB1S1%2CNItqLcdHnpIKp4G
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

<http://192.168.145.128/>

Verified

- **jQuery 1.12.4**

- URL: <http://192.168.145.128/openemr/public/assets/jquery-ui/external/jquery/jquery.js>
- Detection method: The library's name and version were determined based on the file's syntax fingerprint, and contents. Acunetix verified the library version and the associated vulnerabilities with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- CVE-ID: CVE-2015-9251, CVE-2020-11022, CVE-2020-11023
- Description: Possible Cross Site Scripting via third-party text/javascript responses (1.12.0-1.12.2 mitigation reverted) / In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. / In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing option elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

- o References:

- <https://github.com/jquery/jquery/issues/2432>
- <https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/>
- <https://mksben.lo.cm/2020/05/jquery3.5.0-xss.html>
- <https://jquery.com/upgrade-guide/3.5/>
- <https://api.jquery.com/jQuery.htmlPrefilter/>
- <https://www.cvedetails.com/cve/CVE-2020-11022/>
- <https://github.com/advisories/GHSA-gxr4-xjj5-5px2>
- <https://www.cvedetails.com/cve/CVE-2020-11023/>
- <https://github.com/advisories/GHSA-jpcq-cgw6-v4j6>

## Request

---

```
GET /openemr/public/assets/jquery-ui/external/jquery/jquery.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/public/assets/jquery-ui/
Cookie: OpenEMR=6WeVd6ZCNQZ1gcdzS-0v%2CJShmKVZumFVDGJv2At8hAWUVeJ3
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

## <http://192.168.145.128/>

Verified

- **jQuery 1.10.2**

- o URL: <http://192.168.145.128/openemr/public/assets/jquery-datetimepicker/jquery.js>
- o Detection method: The library's name and version were determined based on the file's syntax fingerprint, and contents. Acunetix verified the library version and the associated vulnerabilities with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- o CVE-ID: CVE-2015-9251, CVE-2020-11022, CVE-2020-11023
- o Description: Possible Cross Site Scripting via third-party text/javascript responses / In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. / In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing option elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.
- o References:
  - <https://github.com/jquery/jquery/issues/2432>
  - <http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/>
  - <https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/>

- <https://mksben.l0.cm/2020/05/jquery3.5.0-xss.html>
- <https://jquery.com/upgrade-guide/3.5/>
- <https://api.jquery.com/jQuery.htmlPrefilter/>
- <https://www.cvedetails.com/cve/CVE-2020-11022/>
- <https://github.com/advisories/GHSA-gxr4-xjj5-5px2>
- <https://www.cvedetails.com/cve/CVE-2020-11023/>
- <https://github.com/advisories/GHSA-jpcq-cgw6-v4j6>

## Request

---

```
GET /openemr/public/assets/jquery-datetimepicker/jquery.js HTTP/1.1
Host: 192.168.145.128
accept: /*
accept-language: en-US
cookie: OpenEMR=SMoagLf26TS1Vx2PDvSGHTEJwG3t9eYeCWJyUPD7WNEu5a8X
Referer: http://192.168.145.128/openemr/public/assets/jquery-datetimepicker/
Accept-Encoding: gzip,deflate,br
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
```

<http://192.168.145.128/>

Verified

- **jQuery UI 1.8.10**

- URL: <http://192.168.145.128/openemr/interface/super/rules/www/js/cdr-multiselect/jquery-ui.min.js>
- Detection method: The library's name and version were determined based on the file's syntax fingerprint, and contents. Acunetix verified the library version and the associated vulnerabilities with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- CVE-ID: CVE-2021-41184
- Description: XSS in the 'of' option of the '.position()' util
- References:
  - <https://blog.jqueryui.com/2021/10/jquery-ui-1-13-0-released/>
  - <https://github.com/jquery/jquery-ui/security/advisories/GHSA-gpqq-952q-5327>

## Request

---

```
GET /openemr/interface/super/rules/www/js/cdr-multiselect/jquery-ui.min.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/interface/login_screen.php
Cookie: OpenEMR=2biStMm-fnsHdYMyYHQGKwzilsysHJvKUerLZszaOGdltFQQ
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
```

Host: 192.168.145.128  
Connection: Keep-alive

## <http://192.168.145.128/>

Verified

- **jQuery UI Dialog 1.8.10**

- URL: <http://192.168.145.128/openemr/interface/super/rules/www/js/cdr-multiselect/jquery-ui.min.js>
- Detection method: The library's name and version were determined based on the file's contents. Acunetix verified the library version and the associated vulnerabilities with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- CVE-ID: CVE-2010-5312, CVE-2016-7103
- Description: Title cross-site scripting vulnerability / XSS in dialog closeText
- References:
  - <http://bugs.jqueryui.com/ticket/6016>
  - <https://nodesecurity.io/advisories/127>
  - <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7103>
  - <https://www.cvedetails.com/cve/CVE-2016-7103/>

## Request

```
GET /openemr/interface/super/rules/www/js/cdr-multiselect/jquery-ui.min.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/interface/login_screen.php
Cookie: OpenEMR=2biStMm-fnsHdYMyYHQGKWzilsysHJvKUerLZszaOGdltFQQ
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

## <http://192.168.145.128/>

Verified

- **jQuery 1.5.1**

- URL: <http://192.168.145.128/openemr/interface/super/rules/www/js/cdr-multiselect/jquery.min.js>
- Detection method: The library's name and version were determined based on the file's syntax fingerprint, and contents. Acunetix verified the library version and the associated vulnerabilities with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- CVE-ID: CVE-2011-4969, CVE-2015-9251, CVE-2020-11022, CVE-2020-11023
- Description: Cross-site scripting (XSS) vulnerability in jQuery before 1.6.3, when using location.hash to select elements, allows remote attackers to inject arbitrary web script or HTML via a crafted tag. / Selector

interpreted as HTML / Possible Cross Site Scripting via third-party text/javascript responses / In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. / In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing option elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

- References:

- <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4969>
- <http://research.insecurelabs.org/jquery/test/>
- <http://bugs.jquery.com/ticket/11290>
- <https://github.com/jquery/jquery/issues/2432>
- <http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/>
- <https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/>
- <https://mksben.l0.cm/2020/05/jquery3.5.0-xss.html>
- <https://jquery.com/upgrade-guide/3.5/>
- <https://api.jquery.com/jQuery.htmlPrefilter/>
- <https://www.cvedetails.com/cve/CVE-2020-11022/>
- <https://github.com/advisories/GHSA-gxr4-xjj5-5px2>
- <https://www.cvedetails.com/cve/CVE-2020-11023/>
- <https://github.com/advisories/GHSA-jpcq-cgw6-v4j6>

## Request

---

```
GET /openemr/interface/super/rules/www/js/cdr-multiselect/jquery.min.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/interface/login_screen.php
Cookie: OpenEMR=2biStMm-fnsHdYMyYHQGKwzilsysHJvKUerLZszaOGdltFQQ
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

<http://192.168.145.128/>

Verified

- **jQuery 1.4.3**

- URL: [http://192.168.145.128/openemr/interface/modules/zend\\_modules/public/js/lib/jquery.treeview-1.4.1/lib/jquery.js](http://192.168.145.128/openemr/interface/modules/zend_modules/public/js/lib/jquery.treeview-1.4.1/lib/jquery.js)
- Detection method: The library's name and version were determined based on the file's syntax fingerprint, and contents. Acunetix verified the library version and the associated vulnerabilities with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.

- CVE-ID: CVE-2011-4969, CVE-2015-9251, CVE-2020-11022, CVE-2020-11023
- Description: Cross-site scripting (XSS) vulnerability in jQuery before 1.6.3, when using location.hash to select elements, allows remote attackers to inject arbitrary web script or HTML via a crafted tag. / Selector interpreted as HTML / Possible Cross Site Scripting via third-party text/javascript responses / In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. / In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing option elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.
- References:
  - <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4969>
  - <http://research.insecurelabs.org/jquery/test/>
  - <http://bugs.jquery.com/ticket/11290>
  - <https://github.com/jquery/jquery/issues/2432>
  - <http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/>
  - <https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/>
  - <https://mksben.l0.cm/2020/05/jquery3.5.0-xss.html>
  - <https://jquery.com/upgrade-guide/3.5/>
  - <https://api.jquery.com/jQuery.htmlPrefilter/>
  - <https://www.cvedetails.com/cve/CVE-2020-11022/>
  - <https://github.com/advisories/GHSA-gxr4-xjj5-5px2>
  - <https://www.cvedetails.com/cve/CVE-2020-11023/>
  - <https://github.com/advisories/GHSA-jpcq-cgw6-v4j6>

## Request

---

```

GET /openemr/interface/modules/zend_modules/public/js/lib/jquery.treeview-1.4.1/lib/jquery.js
HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/interface/login_screen.php
Cookie: OpenEMR=2biStMm-fnsHdYMyYHQGKWzilsysHJvKUerLZszaOGdltFQQ
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive

```

<http://192.168.145.128/>

Verified

- jQuery UI 1.11.4
  - URL: [http://192.168.145.128/openemr/interface/forms/eye\\_mag/js/jquery-ui-1-11-4/jquery-ui.min.js](http://192.168.145.128/openemr/interface/forms/eye_mag/js/jquery-ui-1-11-4/jquery-ui.min.js)

- Detection method: The library's name and version were determined based on the file's syntax fingerprint, and contents. Acunetix verified the library version and the associated vulnerabilities with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- CVE-ID: CVE-2021-41184
- Description: XSS in the 'of' option of the '.position()' util
- References:
  - <https://blog.jqueryui.com/2021/10/jquery-ui-1-13-0-released/>
  - <https://github.com/jquery/jquery-ui/security/advisories/GHSA-gpqq-952q-5327>

## Request

---

```
GET /openemr/interface/forms/eye_mag/js/jquery-ui-1-11-4/jquery-ui.min.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/interface/login_screen.php
Cookie: OpenEMR=2biStMm-fnsHdYMyYHQGKWzilsysHJvKUerLZszaOGdltFQQ
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

<http://192.168.145.128/>

Verified

### • jQuery UI Dialog 1.11.4

- URL: [http://192.168.145.128/openemr/interface/forms/eye\\_mag/js/jquery-ui-1-11-4/jquery-ui.min.js](http://192.168.145.128/openemr/interface/forms/eye_mag/js/jquery-ui-1-11-4/jquery-ui.min.js)
- Detection method: The library's name and version were determined based on the file's contents. Acunetix verified the library version and the associated vulnerabilities with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- CVE-ID: CVE-2016-7103
- Description: XSS in dialog closeText
- References:
  - <https://nodesecurity.io/advisories/127>
  - <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7103>
  - <https://www.cvedetails.com/cve/CVE-2016-7103/>

## Request

---

```
GET /openemr/interface/forms/eye_mag/js/jquery-ui-1-11-4/jquery-ui.min.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/interface/login_screen.php
```

Cookie: OpenEMR=2biStMm-fnsHdYMyYHQGKWzilsysHJvKUerLZszaOGdltFQQ  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
Accept-Encoding: gzip,deflate,br  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)  
Chrome/109.0.0.0 Safari/537.36  
Host: 192.168.145.128  
Connection: Keep-alive

## <http://192.168.145.128/> Verified

- **jQuery 1.8.0**

- URL: [http://192.168.145.128/openemr/interface/modules/zend\\_modules/public/js/lib/jquery-1.8.0.min.js](http://192.168.145.128/openemr/interface/modules/zend_modules/public/js/lib/jquery-1.8.0.min.js)
- Detection method: The library's name and version were determined based on the file's name, and contents. Acunetix verified the library version and the associated vulnerabilities with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- CVE-ID: CVE-2015-9251, CVE-2020-11022, CVE-2020-11023
- Description: Selector interpreted as HTML / Possible Cross Site Scripting via third-party text/javascript responses / In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. / In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing option elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.
- References:
  - <http://bugs.jquery.com/ticket/11290>
  - <http://research.insecurelabs.org/jquery/test/>
  - <https://github.com/jquery/jquery/issues/2432>
  - <http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/>
  - <https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/>
  - <https://mksben.l0.cm/2020/05/jquery3.5.0-xss.html>
  - <https://jquery.com/upgrade-guide/3.5/>
  - <https://api.jquery.com/jQuery.htmlPrefilter/>
  - <https://www.cvedetails.com/cve/CVE-2020-11022/>
  - <https://github.com/advisories/GHSA-gxr4-xjj5-5px2>
  - <https://www.cvedetails.com/cve/CVE-2020-11023/>
  - <https://github.com/advisories/GHSA-jpcq-cgw6-v4j6>

## Request

```
GET /openemr/interface/modules/zend_modules/public/js/lib/jquery-1.8.0.min.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/interface/login_screen.php
Cookie: OpenEMR=2biStMm-fnsHdYMyYHQGKWzilsysHJvKUerLZszaOGdltFQQ
```

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
Accept-Encoding: gzip,deflate,br  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)  
Chrome/109.0.0.0 Safari/537.36  
Host: 192.168.145.128  
Connection: Keep-alive

## <http://192.168.145.128/>

Verified

- jQuery 1.8.2

- URL: [http://192.168.145.128/openemr/interface/modules/zend\\_modules/public/js/lib/jquery-1.8.2.min.js](http://192.168.145.128/openemr/interface/modules/zend_modules/public/js/lib/jquery-1.8.2.min.js)
- Detection method: The library's name and version were determined based on the file's name, and contents. Acunetix verified the library version and the associated vulnerabilities with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- CVE-ID: CVE-2015-9251, CVE-2020-11022, CVE-2020-11023
- Description: Selector interpreted as HTML / Possible Cross Site Scripting via third-party text/javascript responses / In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. / In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing option elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.
- References:
  - <http://bugs.jquery.com/ticket/11290>
  - <http://research.insecurelabs.org/jquery/test/>
  - <https://github.com/jquery/jquery/issues/2432>
  - <http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/>
  - <https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/>
  - <https://mksben.lo.cm/2020/05/jquery3.5.0-xss.html>
  - <https://jquery.com/upgrade-guide/3.5/>
  - <https://api.jquery.com/jQuery.htmlPrefilter/>
  - <https://www.cvedetails.com/cve/CVE-2020-11022/>
  - <https://github.com/advisories/GHSA-gxr4-xjj5-5px2>
  - <https://www.cvedetails.com/cve/CVE-2020-11023/>
  - <https://github.com/advisories/GHSA-jpcq-cgw6-v4j6>

## Request

---

GET /openemr/interface/modules/zend\_modules/public/js/lib/jquery-1.8.2.min.js HTTP/1.1  
Acunetix-Aspect: enabled  
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7  
Acunetix-Aspect-ScanID: 1655702786608078775  
Acunetix-Aspect-Queries: aspectalerts;routes  
Referer: http://192.168.145.128/openemr/interface/login\_screen.php  
Cookie: OpenEMR=2biStMm-fnsHdYMyYHQGKWzilsysHJvKUerLZszaOGdltFQQ  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Encoding: gzip, deflate, br  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)  
Chrome/109.0.0.0 Safari/537.36  
Host: 192.168.145.128  
Connection: Keep-alive

## <http://192.168.145.128/> Verified

- **jQuery 1.8.3**

- URL: [http://192.168.145.128/openemr/interface/modules/zend\\_modules/public/js/lib/jquery-1.8.3.js](http://192.168.145.128/openemr/interface/modules/zend_modules/public/js/lib/jquery-1.8.3.js)
- Detection method: The library's name and version were determined based on the file's name, and contents. Acunetix verified the library version and the associated vulnerabilities with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- CVE-ID: CVE-2015-9251, CVE-2020-11022, CVE-2020-11023
- Description: Selector interpreted as HTML / Possible Cross Site Scripting via third-party text/javascript responses / In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. / In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing option elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.
- References:
  - <http://bugs.jquery.com/ticket/11290>
  - <http://research.insecurelabs.org/jquery/test/>
  - <https://github.com/jquery/jquery/issues/2432>
  - <http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/>
  - <https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/>
  - <https://mksben.l0.cm/2020/05/jquery3.5.0-xss.html>
  - <https://jquery.com/upgrade-guide/3.5/>
  - <https://api.jquery.com/jQuery.htmlPrefilter/>
  - <https://www.cvedetails.com/cve/CVE-2020-11022/>
  - <https://github.com/advisories/GHSA-gxr4-xjj5-5px2>
  - <https://www.cvedetails.com/cve/CVE-2020-11023/>
  - <https://github.com/advisories/GHSA-jpcq-cgw6-v4j6>

## Request

---

```
GET /openemr/interface/modules/zend_modules/public/js/lib/jquery-1.8.3.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58adee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/interface/login_screen.php
Cookie: OpenEMR=2biStMm-fnsHdYMyYHQGKwzilsysHJvKUerLZszaOGdltFQQ
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
```

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)  
Chrome/109.0.0.0 Safari/537.36  
Host: 192.168.145.128  
Connection: Keep-alive

## <http://192.168.145.128/>

Confidence: 80%

- **jQuery UI 1.9.2**
  - URL: [http://192.168.145.128/openemr/interface/modules/zend\\_modules/public/js/lib/jquery-ui.custom.js](http://192.168.145.128/openemr/interface/modules/zend_modules/public/js/lib/jquery-ui.custom.js)
  - Detection method: The library's name and version were determined based on the file's contents. Acunetix performed a syntax analysis of the file and detected functional differences between the file and the original library version. As the file was likely modified on purpose, the confidence level of the vulnerability alert has been lowered.
  - CVE-ID: [CVE-2021-41184](#)
  - Description: XSS in the 'of' option of the '.position()' util
  - References:
    - <https://blog.jqueryui.com/2021/10/jquery-ui-1-13-0-released/>
    - <https://github.com/jquery/jquery-ui/security/advisories/GHSA-gpqq-952q-5327>

## Request

GET /openemr/interface/modules/zend\_modules/public/js/lib/jquery-ui.custom.js HTTP/1.1  
Acunetix-Aspect: enabled  
Acunetix-Aspect-Password: d4d608fef00a58adee3950d33ced68a7  
Acunetix-Aspect-ScanID: 1655702786608078775  
Acunetix-Aspect-Queries: aspectalerts;routes  
Referer: http://192.168.145.128/openemr/interface/login\_screen.php  
Cookie: OpenEMR=2biStMm-fnsHdYMyYHQGKwzilsysHJvKUerLZszaOGdltFQQ  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
Accept-Encoding: gzip,deflate,br  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)  
Chrome/109.0.0.0 Safari/537.36  
Host: 192.168.145.128  
Connection: Keep-alive

## <http://192.168.145.128/>

Confidence: 95%

- **jQuery UI Datepicker 1.9.2**
  - URL: [http://192.168.145.128/openemr/interface/modules/zend\\_modules/public/js/lib/jquery-ui.custom.js](http://192.168.145.128/openemr/interface/modules/zend_modules/public/js/lib/jquery-ui.custom.js)
  - Detection method: The library's name and version were determined based on the file's contents.
  - CVE-ID: [CVE-2021-41182](#), [CVE-2021-41183](#)
  - Description: XSS in the 'altField' option of the Datepicker widget / XSS in '\*Text' options of the Datepicker widget
  - References:

- <https://blog.jqueryui.com/2021/10/jquery-ui-1-13-0-released/>
- <https://github.com/jquery/jquery-ui/security/advisories/GHSA-9gj3-hwp5-pmw>
- <https://github.com/jquery/jquery-ui/security/advisories/GHSA-j7qv-pgf6-hvh4>

## Request

---

```
GET /openemr/interface/modules/zend_modules/public/js/lib/jquery-ui.custom.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/interface/login_screen.php
Cookie: OpenEMR=2biStMm-fnsHdYMyYHQGKWzilsysHJvKUerLZszaOGdltFQQ
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

**http://192.168.145.128/**

Verified

- **jQuery UI 1.10.3**

- URL: [http://192.168.145.128/openemr/interface/modules/zend\\_modules/public/js/lib/jquery-ui.js](http://192.168.145.128/openemr/interface/modules/zend_modules/public/js/lib/jquery-ui.js)
- Detection method: The library's name and version were determined based on the file's syntax fingerprint, and contents. Acunetix verified the library version and the associated vulnerabilities with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- CVE-ID: CVE-2021-41184
- Description: XSS in the 'of' option of the '.position()' util
- References:
  - <https://blog.jqueryui.com/2021/10/jquery-ui-1-13-0-released/>
  - <https://github.com/jquery/jquery-ui/security/advisories/GHSA-gpqq-952q-5327>

## Request

---

```
GET /openemr/interface/modules/zend_modules/public/js/lib/jquery-ui.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/interface/login_screen.php
Cookie: OpenEMR=2biStMm-fnsHdYMyYHQGKWzilsysHJvKUerLZszaOGdltFQQ
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
```

<http://192.168.145.128/>

Verified

- jQuery UI Dialog 1.10.3

- URL: http://192.168.145.128/openemr/interface/modules/zend\_modules/public/js/lib/jquery-ui.js
- Detection method: The library's name and version were determined based on the file's contents. Acunetix verified the library version and the associated vulnerabilities with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- CVE-ID: CVE-2016-7103
- Description: XSS in dialog closeText
- References:
  - <https://nodesecurity.io/advisories/127>
  - <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7103>
  - <https://www.cvedetails.com/cve/CVE-2016-7103/>

## Request

---

```
GET /openemr/interface/modules/zend_modules/public/js/lib/jquery-ui.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/interface/login_screen.php
Cookie: OpenEMR=2biStMm-fnsHdYMyYHQGKWzilsysHJvKUerLZszaOGdltFQQ
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

<http://192.168.145.128/>

Confidence: 95%

- jQuery UI Datepicker 1.10.3

- URL: http://192.168.145.128/openemr/interface/modules/zend\_modules/public/js/lib/jquery-ui.js
- Detection method: The library's name and version were determined based on the file's contents.
- CVE-ID: CVE-2021-41182, CVE-2021-41183
- Description: XSS in the 'altField' option of the Datepicker widget / XSS in '\*Text' options of the Datepicker widget
- References:
  - <https://blog.jqueryui.com/2021/10/jquery-ui-1-13-0-released/>
  - <https://github.com/jquery/jquery-ui/security/advisories/GHSA-9gj3-hwp5-pmwc>
  - <https://github.com/jquery/jquery-ui/security/advisories/GHSA-j7qv-pgf6-hvh4>

## Request

---

```
GET /openemr/interface/modules/zend_modules/public/js/lib/jquery-ui.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/interface/login_screen.php
Cookie: OpenEMR=2biStMm-fnsHdYMyYHQGKwzilsysHJvKUerLZszaOGdltFQQ
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

## Recommendation

---

Upgrade to the latest version.

## Outdated JavaScript libraries

---

You are using an outdated version of one or more JavaScript libraries. A more recent version is available. Although your version was not found to be affected by any security vulnerabilities, it is recommended to keep libraries up to date.

### CWE

CWE-937

### CVSS2

AV:N/AC:H/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	High
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

### CVSS3

CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	High
Privileges Required	None
User Interaction	Required
Scope	Changed
Confidentiality	None
Integrity Impact	None
Availability Impact	None

## Impact

---

## <http://10.10.236.31/>

Verified

- **jQuery UI Dialog 1.12.1**

- URL: <http://10.10.236.31/openemr/public/assets/jquery-ui/jquery-ui.js>
- Detection method: The library's name and version were determined based on the file's contents. Acunetix verified the library version with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- References:
  - <https://jqueryui.com/download/>

### Request

```
GET /openemr/public/assets/jquery-ui/jquery-ui.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 8595e182db21cbbc10c83c2c4cf193d3
Acunetix-Aspect-ScanID: 816589585389164376
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://10.10.236.31/openemr/Documentation/help_files/openemr_installation_help.php
Cookie: OpenEMR=b3DHM9s5BR72IjC3y6GcpBb736abtMj3%2CfzaSNeoS-j94pMx
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 10.10.236.31
Connection: Keep-alive
```

## <http://10.10.236.31/>

Verified

- **jQuery UI Tooltip 1.12.1**

- URL: <http://10.10.236.31/openemr/public/assets/jquery-ui/jquery-ui.js>
- Detection method: The library's name and version were determined based on the file's contents. Acunetix verified the library version with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- References:
  - <https://jqueryui.com/download/>

### Request

```
GET /openemr/public/assets/jquery-ui/jquery-ui.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 8595e182db21cbbc10c83c2c4cf193d3
Acunetix-Aspect-ScanID: 816589585389164376
Acunetix-Aspect-Queries: aspectalerts;routes
```

Referer: http://10.10.236.31/openemr/Documentation/help\_files/openemr\_installation\_help.php  
Cookie: OpenEMR=b3DHM9s5BR72IjC3y6GcpBb736abtMj3%2CfzaSNeoS-j94pMx  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
Accept-Encoding: gzip,deflate,br  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)  
Chrome/109.0.0.0 Safari/537.36  
Host: 10.10.236.31  
Connection: Keep-alive

## <http://192.168.145.128/>

Verified

- **jQuery UI Dialog 1.12.1**

- URL: <http://192.168.145.128/openemr/public/assets/jquery-ui/jquery-ui.js>
- Detection method: The library's name and version were determined based on the file's contents. Acunetix verified the library version with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- References:
  - <https://jqueryui.com/download/>

## Request

---

GET /openemr/public/assets/jquery-ui/jquery-ui.js HTTP/1.1  
Acunetix-Aspect: enabled  
Acunetix-Aspect-Password: d4d608fef00a58adee3950d33ced68a7  
Acunetix-Aspect-ScanID: 1655702786608078775  
Acunetix-Aspect-Queries: aspectalerts;routes  
Referer: http://192.168.145.128/openemr/Documentation/help\_files/openemr\_installation\_help.php  
Cookie: OpenEMR=d40D5DeY1SqGsuSImcMvd1XbnUvSB1Sl%2CNItqLcdHnpIKp4G  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
Accept-Encoding: gzip,deflate,br  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)  
Chrome/109.0.0.0 Safari/537.36  
Host: 192.168.145.128  
Connection: Keep-alive

## <http://192.168.145.128/>

Verified

- **jQuery UI Tooltip 1.12.1**

- URL: <http://192.168.145.128/openemr/public/assets/jquery-ui/jquery-ui.js>
- Detection method: The library's name and version were determined based on the file's contents. Acunetix verified the library version with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- References:
  - <https://jqueryui.com/download/>

## Request

---

```
GET /openemr/public/assets/jquery-ui/jquery-ui.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58ad3e3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/Documentation/help_files/openemr_installation_help.php
Cookie: OpenEMR=d40D5DeY1SqGsuSImcMvd1XbnUvSB1S1%2CNItgLcdHnpIKp4G
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

## <http://192.168.145.128/>

Verified

- **jQuery UI Tooltip 1.11.4**

- URL: [http://192.168.145.128/openemr/interface/forms/eye\\_mag/js/jquery-ui-1-11-4/jquery-ui.min.js](http://192.168.145.128/openemr/interface/forms/eye_mag/js/jquery-ui-1-11-4/jquery-ui.min.js)
- Detection method: The library's name and version were determined based on the file's contents. Acunetix verified the library version with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- References:
  - <https://jqueryui.com/download/>

## Request

---

```
GET /openemr/interface/forms/eye_mag/js/jquery-ui-1-11-4/jquery-ui.min.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58ad3e3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/interface/login_screen.php
Cookie: OpenEMR=2biStMm-fnsHdYMyYHQGKwzilsysHJvKUerLZszaOGdltFQQ
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

## <http://192.168.145.128/>

Verified

- **jQuery UI Tooltip 1.10.3**

- URL: [http://192.168.145.128/openemr/interface/modules/zend\\_modules/public/js/lib/jquery-ui.js](http://192.168.145.128/openemr/interface/modules/zend_modules/public/js/lib/jquery-ui.js)
- Detection method: The library's name and version were determined based on the file's contents. Acunetix verified the library version with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- References:
  - <https://jqueryui.com/download/>

## Request

---

```
GET /openemr/interface/modules/zend_modules/public/js/lib/jquery-ui.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/interface/login_screen.php
Cookie: OpenEMR=2biStMm-fnsHdYMyYHQGKwzilsysHJvKUerLZszaOGdltFQQ
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

## <http://192.168.145.128/>

Confidence: 95%

- **Modernizr 2.6.2**

- URL: [http://192.168.145.128/openemr/interface/modules/zend\\_modules/public/js/lib/modernizr-2.6.2.min.js](http://192.168.145.128/openemr/interface/modules/zend_modules/public/js/lib/modernizr-2.6.2.min.js)
- Detection method: The library's name and version were determined based on the file's name.
- References:
  - <https://github.com/Modernizr/Modernizr/releases>

## Request

---

```
GET /openemr/interface/modules/zend_modules/public/js/lib/modernizr-2.6.2.min.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/interface/login_screen.php
Cookie: OpenEMR=2biStMm-fnsHdYMyYHQGKwzilsysHJvKUerLZszaOGdltFQQ
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

## Recommendation

Upgrade to the latest version.

# SC-2 APPLICATION PARTITIONING

The information system separates user functionality (including user interface services) from information system management functionality.

No alerts in this category

# SC-4 INFORMATION IN SHARED RESOURCES

The information system prevents unauthorized and unintended information transfer via shared system resources.

## Development configuration files

One or more configuration files (e.g. Vagrantfile, Gemfile, Rakefile, ...) were found. These files may expose sensitive information that could help a malicious user to prepare more advanced attacks. It's recommended to remove or restrict access to this type of files from production systems.

### CWE

CWE-538

### CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

### CVSS3

CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N

Base Score	3.1
Attack Vector	Network
Attack Complexity	High
Privileges Required	None
User Interaction	Required
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

## Impact

---

These files may disclose sensitive information. This information can be used to launch further attacks.

### <http://10.10.236.31/>

Development configuration files:

- <http://10.10.236.31/openemr/package.json>

package.json => Grunt configuration file. Grunt is a JavaScript task runner.

- <http://10.10.236.31/openemr/composer.json>

composer.json => Composer configuration file. Composer is a dependency manager for PHP.

- <http://10.10.236.31/openemr/composer.lock>

composer.lock => Composer lock file. Composer is a dependency manager for PHP.

- <http://10.10.236.31/openemr/package-lock.json>

package-lock.json => npm file. This file keeps track of the exact version of every package that is installed.

- <http://10.10.236.31/openemr/public/assets/knockout/package.json>

package.json => Grunt configuration file. Grunt is a JavaScript task runner.

## Request

---

```
GET /openemr/package.json HTTP/1.1
Cookie: OpenEMR=bbs8OgzIFbvo7hR%2Cj5ZvMq%2C3QTQmauASLmo3p3YX9WgoZJp2
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 10.10.236.31
Connection: Keep-alive
```

### <http://192.168.145.128/>

Development configuration files:

- <http://192.168.145.128/openemr/package.json>

package.json => Grunt configuration file. Grunt is a JavaScript task runner.

- <http://192.168.145.128/openemr/composer.json>

composer.json => Composer configuration file. Composer is a dependency manager for PHP.

- <http://192.168.145.128/openemr/composer.lock>

composer.lock => Composer lock file. Composer is a dependency manager for PHP.

- <http://192.168.145.128/openemr/package-lock.json>

package-lock.json => npm file. This file keeps track of the exact version of every package that is installed.

- <http://192.168.145.128/openemr/public/assets/jquery-datetimepicker/package.json>

package.json => Grunt configuration file. Grunt is a JavaScript task runner.

- <http://192.168.145.128/openemr/public/assets/jquery-datetimepicker/bower.json>

bower.json => Bower manifest file. Bower is a package manager for the web.

## Request

---

```
GET /openemr/package.json HTTP/1.1
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

## Recommendation

---

Remove or restrict access to all configuration files accessible from internet.

## Directory listings

---

Directory listing is a web server function that displays the directory contents when there is no index file in a specific website directory. It is dangerous to leave this function turned on for the web server because it leads to information disclosure.

### CWE

CWE-538

### CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

### CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

## Impact

A user can view a list of all files from the affected directories possibly exposing sensitive information.

<http://10.10.236.31/>

Verified

Folders with directory listing enabled:

- http://10.10.236.31/openemr/interface/
- http://10.10.236.31/openemr/interface/login/
- http://10.10.236.31/openemr/public/assets/moment/min/
- http://10.10.236.31/openemr/public/assets/knockout/build/output/
- http://10.10.236.31/openemr/public/
- http://10.10.236.31/openemr/interface/main/
- http://10.10.236.31/openemr/public/assets/i18next/dist/umd/
- http://10.10.236.31/openemr/public/assets/knockout/
- http://10.10.236.31/openemr/public/assets/knockout/build/
- http://10.10.236.31/openemr/library/js/
- http://10.10.236.31/openemr/Documentation/
- http://10.10.236.31/openemr/Documentation/help\_files/
- http://10.10.236.31/openemr/public/assets/hotkeys-js/
- http://10.10.236.31/openemr/public/assets/hotkeys-js/dist/
- http://10.10.236.31/openemr/library/js/vendors/
- http://10.10.236.31/openemr/library/js/vendors/validate/
- http://10.10.236.31/openemr/public/assets/jquery-datetimepicker/build/
- http://10.10.236.31/openemr/interface/main/messages/css/
- http://10.10.236.31/openemr/public/assets/jquery/
- http://10.10.236.31/openemr/interface/main/dated\_reminders/
- http://10.10.236.31/openemr/interface/product\_registration/

## Request

```
GET /openemr/interface/ HTTP/1.1
Cookie: OpenEMR=bbs8OgzIFbvo7hR%2Cj5ZvMq%2C3QTQmauASLmo3p3YX9WgoZJp2
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 10.10.236.31
Connection: Keep-alive
```

**http://192.168.145.128/**

Verified

Folders with directory listing enabled:

- <http://192.168.145.128/openemr/interface/>
- <http://192.168.145.128/openemr/interface/login/>
- <http://192.168.145.128/openemr/interface/main/messages/css/>
- <http://192.168.145.128/openemr/public/assets/>
- <http://192.168.145.128/openemr/public/assets/bootstrap/dist/js/>
- <http://192.168.145.128/openemr/interface/main/messages/js/>
- <http://192.168.145.128/openemr/public/assets/moment/>
- <http://192.168.145.128/openemr/library/ajax/>
- [http://192.168.145.128/openemr/interface/main/dated\\_reminders/](http://192.168.145.128/openemr/interface/main/dated_reminders/)
- <http://192.168.145.128/openemr/public/assets/select2/dist/css/>
- <http://192.168.145.128/openemr/public/assets/moment/min/>
- [http://192.168.145.128/openemr/interface/product\\_registration/](http://192.168.145.128/openemr/interface/product_registration/)
- <http://192.168.145.128/openemr/Documentation/>
- <http://192.168.145.128/openemr/public/assets/bootstrap/dist/>
- <http://192.168.145.128/openemr/interface/main/tabs/js/>
- <http://192.168.145.128/openemr/public/assets/i18next/dist/>
- <http://192.168.145.128/openemr/public/assets/i18next/dist/umd/>
- <http://192.168.145.128/openemr/public/>
- <http://192.168.145.128/openemr/public/assets/i18next/>
- <http://192.168.145.128/openemr/public/assets/knockout/>
- <http://192.168.145.128/openemr/public/assets/hotkeys-js/dist/>

## Request

```
GET /openemr/interface/ HTTP/1.1
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

## Recommendation

You should make sure no sensitive information is disclosed or you may want to restrict directory listings from the web server configuration.

## Description

### How to disable directory listings

The easiest way to disable directory listing is to create an index file. The name of the index file depends on the web server configuration. On Apache is called index.htm, index.html. On IIS is named default.asp, default.aspx, default.htm.

On IIS directory listings are disabled by default.

For Apache you need to edit the Apache configuration file (usually named httpd.conf) or create an .htaccess file. In the configuration file you will have the definition of the directory. Something like

```
<Directory /directoryname/subdirectory> Options Indexes FollowSymLinks ...</Directory>
```

To disable directory listing for that directory you need to remove the 'Indexes' option.

## References

### [CWE-548: Exposure of Information Through Directory Listing](#)

<https://cwe.mitre.org/data/definitions/548.html>

## Documentation files

One or more documentation files (e.g. readme.txt, changelog.txt, ...) were found. The information contained in these files could help an attacker identify the web application you are using and sometimes the version of the application. It's recommended to remove these files from production systems.

### CWE

CWE-538

### CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

### CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged

<b>Confidentiality</b>	Low
<b>Integrity Impact</b>	None
<b>Availability Impact</b>	None

## Impact

---

These files may disclose sensitive information. This information can be used to launch further attacks.

### <http://10.10.236.31/>

Documentation files:

- <http://10.10.236.31/openemr/README.md>

File contents (first 100 characters):

```
! [Syntax Status] (https://github.com/openemr/openemr/workflows/Syntax/badge.svg?branch=rel-700)
! [Sty ...
```

- <http://10.10.236.31/openemr/interface/README.md>

File contents (first 100 characters):

```
# OpenEMR-interface
```

```
The OpenEMR UI is built with [SASS] (https://sass-lang.com/) on top of a bootstr
...

```

- <http://10.10.236.31/openemr/public/assets/knockout/README.md>

File contents (first 100 characters):

```
# Knockout
```

```
**Knockout** is a JavaScript [MVVM]
(https://en.wikipedia.org/wiki/Model\_View\_ViewModel) ...
```

## Request

---

```
GET /openemr/README.md HTTP/1.1
Cookie: OpenEMR=bbs8OgzIFbvo7hR%2Cj5ZvMq%2C3QTQmauASLmo3p3YX9WgoZJp2
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 10.10.236.31
Connection: Keep-alive
```

## <http://192.168.145.128/>

Documentation files:

- <http://192.168.145.128/openemr/README.md>

File contents (first 100 characters):

```
! [Syntax Status] (https://github.com/openemr/openemr/workflows/Syntax/badge.svg?branch=rel-700)
! [Sty ...
```

- <http://192.168.145.128/openemr/interface/README.md>

File contents (first 100 characters):

```
# OpenEMR-interface
```

```
The OpenEMR UI is built with [SASS] (https://sass-lang.com/) on top of a bootstr
...
```

- <http://192.168.145.128/openemr/public/assets/jquery-datetimepicker/README.md>

File contents (first 100 characters):

```
# jQuery DateTimePicker
[Demo and Documentation] (https://xdsoft.net/jqplugins/datetimepicker/)
```

```
[ ! [B ...
```

## Request

```
GET /openemr/README.md HTTP/1.1
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

## Recommendation

Remove or restrict access to all documentation file accessible from internet.

## Application error messages

This alert requires manual confirmation

Acunetix found one or more error/warning messages. Application error or warning messages may expose

sensitive information about an application's internal workings to an attacker. These messages may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page(s).

## CWE

CWE-209

## CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

## CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

## Impact

Error messages may disclose sensitive information which can be used to escalate attacks.

## <http://10.10.236.31/>

Application error messages:

- http://10.10.236.31/openemr/interface/main/main\_screen.php  
**Unknown column 'Array' in 'where clause'**
- http://10.10.236.31/openemr/interface/main/main\_screen.php  
**<b>Warning</b>: include\_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php): failed to open stream: No such file or directory in <b>/var/www/html/openemr/interface/main/main\_screen.php</b> on line <b>5137</b><br />**
- http://10.10.236.31/openemr/interface/main/main\_screen.php  
**<b>Warning</b>: include\_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion (include\_path='/var/www/html/openemr/vendor/pear/archive\_tar:/var/www/html/openemr/vendor/pear/cole\_getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear\_exception:::/usr/share/php') in <b>/var/www/html/openemr/interface/main/main\_screen.php</b> on line <b>5137</b><br />**

- http://10.10.236.31/openemr/interface/main/main\_screen.php  
**Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion**
- http://10.10.236.31/openemr/interface/main/messages/messages.php  
**<b>Warning</b>: include\_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php): failed to open stream: No such file or directory in <b>/var/www/html/openemr/interface/main/messages/messages.php</b> on line <b>5137</b><br />**
- http://10.10.236.31/openemr/interface/main/messages/messages.php  
**<b>Warning</b>: include\_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion (include\_path='/var/www/html/openemr/vendor/pear/archive\_tar:/var/www/html/openemr/vendor/pear/cole\_getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear\_exception:::/usr/share/php') in <b>/var/www/html/openemr/interface/main/messages/messages.php</b> on line <b>5137</b><br />**
- http://10.10.236.31/openemr/interface/main/messages/messages.php  
**Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion**
- http://10.10.236.31/openemr/library/ajax/dated\_reminders\_counter.php  
**<b>Warning</b>: include\_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php): failed to open stream: No such file or directory in <b>/var/www/html/openemr/library/ajax/dated\_reminders\_counter.php</b> on line <b>5137</b><br />**
- http://10.10.236.31/openemr/library/ajax/dated\_reminders\_counter.php  
**<b>Warning</b>: include\_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion (include\_path='/var/www/html/openemr/vendor/pear/archive\_tar:/var/www/html/openemr/vendor/pear/cole\_getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear\_exception:::/usr/share/php') in <b>/var/www/html/openemr/library/ajax/dated\_reminders\_counter.php</b> on line <b>5137</b><br />**
- http://10.10.236.31/openemr/library/ajax/dated\_reminders\_counter.php  
**Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion**
- http://10.10.236.31/openemr/library/ajax/i18n\_generator.php  
**<b>Warning</b>: include\_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php): failed to open stream: No such file or directory in <b>/var/www/html/openemr/library/ajax/i18n\_generator.php</b> on line <b>5137</b><br />**
- http://10.10.236.31/openemr/library/ajax/i18n\_generator.php  
**<b>Warning</b>: include\_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion**

```
(include_path='/var/www/html/openemr/vendor/pear/archive_tar:/var/www/html/openemr/vendor/pear/console_getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear_exception:::/usr/share/php') in  
<b>/var/www/html/openemr/library/ajax/i18n_generator.php</b> on line <b>5137</b><br />
```

- http://10.10.236.31/openemr/library/ajax/i18n\_generator.php  
**Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion**
- http://10.10.236.31/openemr/interface/main/calendar/index.php  
**<b>Warning</b>: include\_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php): failed to open stream: No such file or directory in**  
**<b>/var/www/html/openemr/interface/main/calendar/index.php</b> on line <b>5137</b><br />**
- http://10.10.236.31/openemr/interface/main/calendar/index.php  
**<b>Warning</b>: include\_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion**  
(include\_path='/var/www/html/openemr/vendor/pear/archive\_tar:/var/www/html/openemr/vendor/pear/console\_getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear\_exception:::/usr/share/php') in  
**<b>/var/www/html/openemr/interface/main/calendar/index.php</b> on line <b>5137</b><br />**
- http://10.10.236.31/openemr/interface/main/calendar/index.php  
**Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion**
- http://10.10.236.31/openemr/interface/login/login.php  
**<b>Warning</b>: include\_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php): failed to open stream: No such file or directory in**  
**<b>/var/www/html/openemr/interface/login/login.php</b> on line <b>5137</b><br />**
- http://10.10.236.31/openemr/interface/login/login.php  
**<b>Warning</b>: include\_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion**  
(include\_path='/var/www/html/openemr/vendor/pear/archive\_tar:/var/www/html/openemr/vendor/pear/console\_getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear\_exception:::/usr/share/php') in  
**<b>/var/www/html/openemr/interface/login/login.php</b> on line <b>5137</b><br />**
- http://10.10.236.31/openemr/interface/login/login.php  
**Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion**
- http://10.10.236.31/openemr/interface/main/tabs/main.php  
**<b>Warning</b>: include\_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-**

mysqli\_log.inc.php): failed to open stream: No such file or directory in  
<b>/var/www/html/openemr/interface/main/tabs/main.php</b> on line <b>5137</b><br />

- http://10.10.236.31/openemr/interface/main/tabs/main.php  
<b>Warning</b>: include\_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb.php/drivers/adodb-mysqli\_log.inc.php' for inclusion  
(include\_path='/var/www/html/openemr/vendor/pear/archive\_tar:/var/www/html/openemr/vendor/pear/console getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear\_exception:::/usr/share/php') in  
<b>/var/www/html/openemr/interface/main/tabs/main.php</b> on line <b>5137</b><br />

## Request

---

```
POST /openemr/interface/main/main_screen.php?auth=login&site=default HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://10.10.236.31/openemr
Cookie: OpenEMR=bbs8OgzIFbvo7hR%2Cj5ZvMq%2C3QTQmauASLmo3p3YX9WgoZJp2
Content-Length: 72
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 10.10.236.31
Connection: Keep-alive

authUser[] = 1&clearPass = 1&languageChoice = 1&new_login_session_management = 1
```

## http://192.168.145.128/

Application error messages:

- http://192.168.145.128/openemr/interface/main/main\_screen.php  
<b>Warning</b>: include\_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php): failed to open stream: No such file or directory in  
<b>/var/www/html/openemr/interface/main/main\_screen.php</b> on line <b>5137</b><br />
- http://192.168.145.128/openemr/interface/main/main\_screen.php  
<b>Warning</b>: include\_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb.php/drivers/adodb-mysqli\_log.inc.php' for inclusion  
(include\_path='/var/www/html/openemr/vendor/pear/archive\_tar:/var/www/html/openemr/vendor/pear/console getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear\_exception:::/usr/share/php') in  
<b>/var/www/html/openemr/interface/main/main\_screen.php</b> on line <b>5137</b><br />
- http://192.168.145.128/openemr/interface/main/main\_screen.php  
Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for

## inclusion

- http://192.168.145.128/openemr/interface/main/messages/messages.php  
**<b>Warning</b>: include\_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php): failed to open stream: No such file or directory in**  
**<b>/var/www/html/openemr/interface/main/messages/messages.php</b> on line <b>5137</b><br />**
- http://192.168.145.128/openemr/interface/main/messages/messages.php  
**<b>Warning</b>: include\_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion**  
(include\_path='/var/www/html/openemr/vendor/pear/archive\_tar:/var/www/html/openemr/vendor/pear/console\_getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear\_exception:::/usr/share/php') in  
**<b>/var/www/html/openemr/interface/main/messages/messages.php</b> on line <b>5137</b><br />**
- http://192.168.145.128/openemr/interface/main/messages/messages.php  
Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion
- http://192.168.145.128/openemr/library/ajax/dated\_reminders\_counter.php  
**<b>Warning</b>: include\_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php): failed to open stream: No such file or directory in**  
**<b>/var/www/html/openemr/library/ajax/dated\_reminders\_counter.php</b> on line <b>5137</b><br />**
- http://192.168.145.128/openemr/library/ajax/dated\_reminders\_counter.php  
**<b>Warning</b>: include\_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion**  
(include\_path='/var/www/html/openemr/vendor/pear/archive\_tar:/var/www/html/openemr/vendor/pear/console\_getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear\_exception:::/usr/share/php') in  
**<b>/var/www/html/openemr/library/ajax/dated\_reminders\_counter.php</b> on line <b>5137</b><br />**
- http://192.168.145.128/openemr/library/ajax/dated\_reminders\_counter.php  
Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion
- http://192.168.145.128/openemr/interface/login/login.php  
**<b>Warning</b>: include\_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php): failed to open stream: No such file or directory in**  
**<b>/var/www/html/openemr/interface/login/login.php</b> on line <b>5137</b><br />**
- http://192.168.145.128/openemr/interface/login/login.php  
**<b>Warning</b>: include\_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion**  
(include\_path='/var/www/html/openemr/vendor/pear/archive\_tar:/var/www/html/openemr/vendor/pear/console\_getopt:/var/www/html/openemr/vendor/pear/pear-core-

minimal/src:/var/www/html/openemr/vendor/pear/pear\_exception:::/usr/share/php') in  
<b>/var/www/html/openemr/interface/login/login.php</b> on line <b>5137</b><br />

- http://192.168.145.128/openemr/interface/login/login.php  
Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion
- http://192.168.145.128/openemr/library/ajax/i18n\_generator.php  
<b>Warning</b>: include\_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php): failed to open stream: No such file or directory in  
<b>/var/www/html/openemr/library/ajax/i18n\_generator.php</b> on line <b>5137</b><br />
- http://192.168.145.128/openemr/library/ajax/i18n\_generator.php  
<b>Warning</b>: include\_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion  
(include\_path='/var/www/html/openemr/vendor/pear/archive\_tar:/var/www/html/openemr/vendor/pear/console\_getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear\_exception:::/usr/share/php') in  
<b>/var/www/html/openemr/library/ajax/i18n\_generator.php</b> on line <b>5137</b><br />
- http://192.168.145.128/openemr/library/ajax/i18n\_generator.php  
Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion
- http://192.168.145.128/openemr/interface/login\_screen.php  
<b>Warning</b>: include\_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php): failed to open stream: No such file or directory in  
<b>/var/www/html/openemr/interface/login\_screen.php</b> on line <b>5137</b><br />
- http://192.168.145.128/openemr/interface/login\_screen.php  
<b>Warning</b>: include\_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion  
(include\_path='/var/www/html/openemr/vendor/pear/archive\_tar:/var/www/html/openemr/vendor/pear/console\_getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear\_exception:::/usr/share/php') in  
<b>/var/www/html/openemr/interface/login\_screen.php</b> on line <b>5137</b><br />
- http://192.168.145.128/openemr/interface/login\_screen.php  
Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion
- http://192.168.145.128/openemr/interface/main/dated\_reminders/dated\_reminders.php  
<b>Warning</b>: include\_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php): failed to open stream: No such file or directory in  
<b>/var/www/html/openemr/interface/main/dated\_reminders/dated\_reminders.php</b> on line <b>5137</b><br />

- http://192.168.145.128/openemr/interface/main/dated\_reminders/dated\_reminders.php  
**<b>Warning</b>: include\_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion**  
**(include\_path='/var/www/html/openemr/vendor/pear/archive\_tar:/var/www/html/openemr/vendor/pear/cole\_getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear\_exception:::/usr/share/php') in**  
**<b>/var/www/html/openemr/interface/main/dated\_reminders/dated\_reminders.php</b> on line <b>5137</b>**  
**<br />**
- http://192.168.145.128/openemr/interface/main/dated\_reminders/dated\_reminders.php  
**Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion**

## Request

---

```
GET /openemr/interface/main/main_screen.php HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: filelist;packages;aspectalerts;routes
Referer: http://192.168.145.128/openemr
Cookie: OpenEMR=fLVw-dnCSU123MMDJ4XDEmokIFFZN%2CUpmA0oNxhYR1Fnqazp
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

## Recommendation

---

Verify that these page(s) are disclosing error or warning messages and properly configure the application to log errors to a file instead of displaying the error to the user.

## Description

---

While information disclosure vulnerabilities are not directly exploitable by an attacker, they may help an attacker to learn about system specific information. The following is a list of **some** of the information an attacker may be able to obtain from application error disclosure.

- Internal IP addresses
- Secrets (passwords, keys, tokens...)
- Operating system distributions
- Software version numbers
- Missing security patches
- Application stack traces
- SQL statements

Location of sensitive files (backups, temporary files...)

Location of sensitive resources (databases, caches, code repositories...)

## References

---

### [PHP Runtime Configuration](#)

<https://www.php.net/manual/en/errorfunc.configuration.php#ini.display-errors>

### [Improper Error Handling](#)

[https://www.owasp.org/index.php/Improper\\_Error\\_Handling](https://www.owasp.org/index.php/Improper_Error_Handling)

## Possible sensitive directories

---

One or more possibly sensitive directories were found. These resources are not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

### CWE

CWE-200

### CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

### CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

## Impact

---

These directories may expose sensitive information that could help a malicious user to prepare more advanced attacks.

### <http://10.10.236.31/>

Possible sensitive directories:

- <http://10.10.236.31/openemr/bin>
- <http://10.10.236.31/openemr/sql>
- <http://10.10.236.31/openemr/config>
- <http://10.10.236.31/openemr/tests>
- <http://10.10.236.31/openemr/src>

## Request

---

```
GET /openemr/bin/ HTTP/1.1
Cookie: OpenEMR=bbs8OgzIFbvo7hR%2Cj5ZvMq%2C3QTQmauASLmo3p3YX9WgoZJp2
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 10.10.236.31
Connection: Keep-alive
```

## <http://192.168.145.128/>

Possible sensitive directories:

- <http://192.168.145.128/openemr/bin>
- <http://192.168.145.128/openemr/sql>
- <http://192.168.145.128/openemr/config>
- <http://192.168.145.128/openemr/tests>
- <http://192.168.145.128/openemr/src>

## Request

---

```
GET /openemr/bin/ HTTP/1.1
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

## Recommendation

---

Restrict access to these directories or remove them from the website.

## References

---

### [Web Server Security and Database Server Security](#)

<https://www.acunetix.com/websitesecurity/webserver-security/>

## Possible sensitive files

---

A possible sensitive file has been found. This file is not directly linked from the website. This check looks for common sensitive resources like password files, configuration files, log files, include files, statistics data, database dumps. Each one of these files could help an attacker to learn more about his target.

### CWE

CWE-200

### CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

### CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

## Impact

---

This file may expose sensitive information that could help a malicious user to prepare more advanced attacks.

### <http://10.10.236.31/>

Possible sensitive files:

- <http://10.10.236.31/openemr/admin.php>

## Request

---

```
GET /openemr/admin.php HTTP/1.1
Accept: ydabcrvp/kkoy
Cookie: OpenEMR=bbs80gzIFbvo7hR%2Cj5ZvMq%2C3QTQmauASLmo3p3YX9WgoZJp2
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 10.10.236.31
Connection: Keep-alive
```

## <http://192.168.145.128/>

Possible sensitive files:

- <http://192.168.145.128/openemr/admin.php>

### Request

---

```
GET /openemr/admin.php HTTP/1.1
Accept: shxrinco/hemy
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

### Recommendation

---

Restrict access to this file or remove it from the website.

### References

---

#### [Web Server Security and Database Server Security](#)

<https://www.acunetix.com/websitesecurity/webserver-security/>

### Email addresses

---

One or more email addresses have been found on this website. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

#### CWE

CWE-200

#### CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:N

#### CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None

<b>Availability Impact</b>	None
----------------------------	------

<b>Scope</b>	Unchanged
<b>Confidentiality</b>	None
<b>Integrity Impact</b>	None
<b>Availability Impact</b>	None

## Impact

---

Email addresses posted on Web sites may attract spam.

### <http://10.10.236.31/>

Emails found:

- [http://10.10.236.31/openemr/acknowledge\\_license\\_cert.html](http://10.10.236.31/openemr/acknowledge_license_cert.html)  
**ajabour@iupui.edu**
- [http://10.10.236.31/openemr/acknowledge\\_license\\_cert.html](http://10.10.236.31/openemr/acknowledge_license_cert.html)  
**andres@paglayan.com**
- [http://10.10.236.31/openemr/acknowledge\\_license\\_cert.html](http://10.10.236.31/openemr/acknowledge_license_cert.html)  
**superarnab@gmail.com**
- [http://10.10.236.31/openemr/acknowledge\\_license\\_cert.html](http://10.10.236.31/openemr/acknowledge_license_cert.html)  
**drbowen@bowenmd.com**
- [http://10.10.236.31/openemr/acknowledge\\_license\\_cert.html](http://10.10.236.31/openemr/acknowledge_license_cert.html)  
**bss@iguanasuicide.net**
- [http://10.10.236.31/openemr/acknowledge\\_license\\_cert.html](http://10.10.236.31/openemr/acknowledge_license_cert.html)  
**brady.g.miller@gmail.com**
- [http://10.10.236.31/openemr/acknowledge\\_license\\_cert.html](http://10.10.236.31/openemr/acknowledge_license_cert.html)  
**pandi.param@capminds.com**
- [http://10.10.236.31/openemr/acknowledge\\_license\\_cert.html](http://10.10.236.31/openemr/acknowledge_license_cert.html)  
**stephen.waite@cmsvt.com**
- [http://10.10.236.31/openemr/acknowledge\\_license\\_cert.html](http://10.10.236.31/openemr/acknowledge_license_cert.html)  
**amit@comlinkinc.com**
- [http://10.10.236.31/openemr/acknowledge\\_license\\_cert.html](http://10.10.236.31/openemr/acknowledge_license_cert.html)  
**sbhayani@communitybehavioralhealth.net**
- [http://10.10.236.31/openemr/acknowledge\\_license\\_cert.html](http://10.10.236.31/openemr/acknowledge_license_cert.html)  
**ramesh@ensoftek.com**
- [http://10.10.236.31/openemr/acknowledge\\_license\\_cert.html](http://10.10.236.31/openemr/acknowledge_license_cert.html)  
**george.tye@gmail.com**
- [http://10.10.236.31/openemr/acknowledge\\_license\\_cert.html](http://10.10.236.31/openemr/acknowledge_license_cert.html)  
**stone@annashaegrp.com**
- [http://10.10.236.31/openemr/acknowledge\\_license\\_cert.html](http://10.10.236.31/openemr/acknowledge_license_cert.html)  
**fndtn357@gmail.com**
- [http://10.10.236.31/openemr/acknowledge\\_license\\_cert.html](http://10.10.236.31/openemr/acknowledge_license_cert.html)  
**sherwin@affordablecustomehr.com**
- [http://10.10.236.31/openemr/acknowledge\\_license\\_cert.html](http://10.10.236.31/openemr/acknowledge_license_cert.html)  
**julia.longtin@gmail.com**

- http://10.10.236.31/openemr/acknowledge\_license\_cert.html  
ptspohnpei@gmail.com
- http://10.10.236.31/openemr/acknowledge\_license\_cert.html  
kevin.y@integralemr.com
- http://10.10.236.31/openemr/acknowledge\_license\_cert.html  
openemr@lillysystems.com
- http://10.10.236.31/openemr/acknowledge\_license\_cert.html  
mscltd@earthlink.net
- http://10.10.236.31/openemr/acknowledge\_license\_cert.html  
mdsupport@users.sf.net

## Request

---

```
GET /openemr/acknowledge_license_cert.html HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 8595e182db21cbbc10c83c2c4cf193d3
Acunetix-Aspect-ScanID: 816589585389164376
Acunetix-Aspect-Queries: packages;aspectalerts;routes
Referer: http://10.10.236.31/openemr/interface/login/login.php
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 10.10.236.31
Connection: Keep-alive
```

## <http://192.168.145.128/>

Emails found:

- http://192.168.145.128/openemr/acknowledge\_license\_cert.html  
ajabour@iupui.edu
- http://192.168.145.128/openemr/acknowledge\_license\_cert.html  
andres@paglayan.com
- http://192.168.145.128/openemr/acknowledge\_license\_cert.html  
superarnab@gmail.com
- http://192.168.145.128/openemr/acknowledge\_license\_cert.html  
drbowen@bowenmd.com
- http://192.168.145.128/openemr/acknowledge\_license\_cert.html  
bss@iguanasuicide.net
- http://192.168.145.128/openemr/acknowledge\_license\_cert.html  
brady.g.miller@gmail.com
- http://192.168.145.128/openemr/acknowledge\_license\_cert.html  
pandi.param@capminds.com
- http://192.168.145.128/openemr/acknowledge\_license\_cert.html  
stephen.waite@cmsvt.com
- http://192.168.145.128/openemr/acknowledge\_license\_cert.html  
amit@comlinkinc.com

- http://192.168.145.128/openemr/acknowledge\_license\_cert.html  
**sbhayani@communitybehavioralhealth.net**
- http://192.168.145.128/openemr/acknowledge\_license\_cert.html  
**ramesh@ensoftek.com**
- http://192.168.145.128/openemr/acknowledge\_license\_cert.html  
**george.tye@gmail.com**
- http://192.168.145.128/openemr/acknowledge\_license\_cert.html  
**stone@annashaegrp.com**
- http://192.168.145.128/openemr/acknowledge\_license\_cert.html  
**fndtn357@gmail.com**
- http://192.168.145.128/openemr/acknowledge\_license\_cert.html  
**sherwin@affordablecustomehr.com**
- http://192.168.145.128/openemr/acknowledge\_license\_cert.html  
**julia.longtin@gmail.com**
- http://192.168.145.128/openemr/acknowledge\_license\_cert.html  
**ptspohnpei@gmail.com**
- http://192.168.145.128/openemr/acknowledge\_license\_cert.html  
**kevin.y@integralemr.com**
- http://192.168.145.128/openemr/acknowledge\_license\_cert.html  
**openemr@lillysystems.com**
- http://192.168.145.128/openemr/acknowledge\_license\_cert.html  
**mscltd@earthlink.net**
- http://192.168.145.128/openemr/acknowledge\_license\_cert.html  
**mdsupport@users.sf.net**

## Request

---

```
GET /openemr/acknowledge_license_cert.html HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/interface/login/login.php
Cookie: OpenEMR=F-6X1PVs1YyH8tuel82CU%2CjzXjI%2C2Xj1wHpg%2CMTJEHOAPWa5
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

## Recommendation

---

Check references for details on how to solve this problem.

## References

---

[Anti-spam techniques](#)

## Error page web server version disclosure

Application errors or warning messages may disclose sensitive information about an application's internal workings to an attacker.

Acunetix found the web server version number and a list of modules enabled on the target server. Consult the 'Attack details' section for more information about the affected page.

### CWE

CWE-200

### CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

### CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

## Impact

Error messages information about an application's internal workings may be used to escalate attacks.

<http://10.10.236.31/>

### Request

```
GET /KnNz3PhQmq HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 10.10.236.31
Connection: Keep-alive
```

## <http://192.168.145.128/>

### Request

---

```
GET /OSEbyESLkq HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

### Recommendation

---

Properly configure the web server not to disclose information about an application's internal workings to the user. Consult the 'Web references' section for more information.

### References

---

#### [Custom Error Responses \(Apache HTTP Server\)](#)

<https://httpd.apache.org/docs/current/custom-error.html>

#### [server\\_tokens \(Nginx\)](#)

[http://nginx.org/en/docs/http/ngx\\_http\\_core\\_module.html#server\\_tokens](http://nginx.org/en/docs/http/ngx_http_core_module.html#server_tokens)

#### [Remove Unwanted HTTP Response Headers \(Microsoft IIS\)](#)

<https://blogs.msdn.microsoft.com/varunm/2013/04/23/remove-unwanted-http-response-headers/>

## Possible server path disclosure (Unix)

---

One or more fully qualified path names were found. From this information the attacker may learn the file system structure from the web server. This information can be used to conduct further attacks.

This alert may be a false positive, manual confirmation is required.

### CWE

CWE-200

### CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial

### CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None

<b>Integrity Impact</b>	None
<b>Availability Impact</b>	None

<b>User Interaction</b>	None
<b>Scope</b>	Unchanged
<b>Confidentiality</b>	Low
<b>Integrity Impact</b>	None
<b>Availability Impact</b>	None

## Impact

---

Possible sensitive information disclosure.

### <http://10.10.236.31/>

Pages with paths being disclosed:

- http://10.10.236.31/openemr/interface/main/main\_screen.php  
(/var/www/html/openemr/vendor/adodb/adodb)
- http://10.10.236.31/openemr/interface/main/messages/messages.php  
(/var/www/html/openemr/vendor/adodb/adodb)
- http://10.10.236.31/openemr/library/ajax/dated\_reminders\_counter.php  
(/var/www/html/openemr/vendor/adodb/adodb)
- http://10.10.236.31/openemr/library/ajax/i18n\_generator.php  
(/var/www/html/openemr/vendor/adodb/adodb)
- http://10.10.236.31/  
  >/var/www/html/index.html
- http://10.10.236.31/openemr/interface/main/calendar/index.php  
(/var/www/html/openemr/vendor/adodb/adodb)
- http://10.10.236.31/openemr/interface/login/login.php  
(/var/www/html/openemr/vendor/adodb/adodb)
- http://10.10.236.31/openemr/interface/main/tabs/main.php  
(/var/www/html/openemr/vendor/adodb/adodb)
- http://10.10.236.31/openemr/interface/main/dated\_reminders/dated\_reminders.php  
(/var/www/html/openemr/vendor/adodb/adodb)
- http://10.10.236.31/openemr/portal/  
  (/var/www/html/openemr/vendor/adodb/adodb)
- http://10.10.236.31/openemr/Documentation/Readme\_edihistory.html  
  (/var/www/htdocs/openemr/sites/)
- http://10.10.236.31/openemr/portal/messaging/secure\_chat.php  
  (/var/www/html/openemr/vendor/adodb/adodb)
- http://10.10.236.31/openemr/Documentation/help\_files/adminacl\_help.php  
  (/var/www/html/openemr/vendor/adodb/adodb)
- http://10.10.236.31/openemr/Documentation/README-Log-Backup.txt  
  (/var/www/openemr)
- http://10.10.236.31/openemr/Documentation/help\_files/cms\_1500\_help.php  
  (/var/www/html/openemr/vendor/adodb/adodb)

- http://10.10.236.31/openemr/Documentation/help\_files/configure\_orders\_help.php  
(/var/www/html/openemr/vendor/adodb/adodb)
- http://10.10.236.31/openemr/library/ajax/imm\_autocomplete/search.php  
(/var/www/html/openemr/vendor/adodb/adodb)
- http://10.10.236.31/openemr/Documentation/help\_files/mfa\_help.php  
(/var/www/html/openemr/vendor/adodb/adodb)
- http://10.10.236.31/openemr/library/ajax/document\_helpers.php  
(/var/www/html/openemr/vendor/adodb/adodb)
- http://10.10.236.31/openemr/interface/login\_screen.php  
(/var/www/html/openemr/vendor/adodb/adodb)
- http://10.10.236.31/openemr/Documentation/help\_files/openemr\_installation\_help.php  
/var/www/html/openemr

## Request

---

```
GET /openemr/interface/main/main_screen.php HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 8595e182db21cbbc10c83c2c4cf193d3
Acunetix-Aspect-ScanID: 816589585389164376
Acunetix-Aspect-Queries: filelist;packages;aspectalerts;routes
Referer: http://10.10.236.31/openemr
Cookie: OpenEMR=Dj68HNoGw-vYWT2k81NHDiqIHhLtRgfoVY0Tqo%2Cj6JeJm5aU
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 10.10.236.31
Connection: Keep-alive
```

## <http://192.168.145.128/>

Pages with paths being disclosed:

- http://192.168.145.128/openemr/interface/main/main\_screen.php  
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/interface/main/messages/messages.php  
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/library/ajax/dated\_reminders\_counter.php  
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/interface/login/login.php  
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/library/ajax/i18n\_generator.php  
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/  
>/var/www/html/index.html
- http://192.168.145.128/openemr/interface/login\_screen.php  
(/var/www/html/openemr/vendor/adodb/adodb)

- http://192.168.145.128/openemr/interface/main/dated\_reminders/dated\_reminders.php  
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/interface/main/tabs/main.php  
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/portal/  
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/portal/messaging/messages.php  
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/portal/messaging/secure\_chat.php  
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/Documentation/Readme\_edihistory.html  
/var/www/htdocs/openemr/sites/
- http://192.168.145.128/openemr/Documentation/help\_files/add\_edit\_transactions\_dashboard\_help.php  
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/Documentation/README-Log-Backup.txt  
/var/www/openemr
- http://192.168.145.128/openemr/Documentation/help\_files/adminacl\_help.php  
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/Documentation/help\_files/cms\_1500\_help.php  
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/library/FeeSheet.class.php  
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/Documentation/help\_files/common\_help.php  
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/library/FeeSheetHtml.class.php  
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/Documentation/help\_files/configure\_orders\_help.php  
(/var/www/html/openemr/vendor/adodb/adodb)

## Request

---

```

GET /openemr/interface/main/main_screen.php HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: filelist;packages;aspectalerts;routes
Referer: http://192.168.145.128/openemr
Cookie: OpenEMR=fLVw-dnCSU123MMDJ4XDEmokIFFZN%2CUpmA0oNxhYR1Fnqazp
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive

```

## Recommendation

---

Prevent this information from being displayed to the user.

## References

---

### [Full Path Disclosure](#)

[https://www.owasp.org/index.php/Full\\_Path\\_Disclosure](https://www.owasp.org/index.php/Full_Path_Disclosure)

## SC-5 DENIAL OF SERVICE PROTECTION

---

The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined list of types of denial of service attacks or reference to source for current list].

No alerts in this category

## SC-8 TRANSMISSION CONFIDENTIALITY AND INTEGRITY

---

The information system protects the integrity of transmitted information.

### User credentials are sent in clear text

---

User credentials are transmitted over an unencrypted channel. This information should always be transferred via an encrypted channel (HTTPS) to avoid being intercepted by malicious users.

#### CWE

CWE-523

#### CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

#### CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N

Base Score	4.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None

Availability Impact	None
---------------------	------

## Impact

---

A third party may be able to read the user credentials by intercepting an unencrypted HTTP connection.

### <http://10.10.236.31/>

Forms with credentials sent in clear text:

- <http://10.10.236.31/openemr/interface/login/login.php>

```
Form name: login_form
Form action: ../main/main_screen.php?auth=login&site=default
Form method: POST
Password input: clearPass
```

## Request

---

```
GET /openemr/interface/login/login.php?site=default HTTP/1.1
Host: 10.10.236.31
Pragma: no-cache
Cache-Control: no-cache
accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
accept-language: en-US
upgrade-insecure-requests: 1
Accept-Encoding: gzip,deflate,br
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
```

### <http://192.168.145.128/>

Forms with credentials sent in clear text:

- <http://192.168.145.128/openemr/interface/login/login.php>

```
Form name: login_form
Form action: ../main/main_screen.php?auth=login&site=default
Form method: POST
Password input: clearPass
```

## Request

---

```
GET /openemr/interface/login/login.php?site=default HTTP/1.1
Host: 192.168.145.128
Pragma: no-cache
Cache-Control: no-cache
accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
accept-language: en-US
upgrade-insecure-requests: 1
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0 Safari/537.36
```

## Recommendation

Because user credentials are considered sensitive information, should always be transferred to the server over an encrypted connection (HTTPS).

## Unencrypted connection

This scan target was connected to over an unencrypted connection. A potential attacker can intercept and modify data sent and received from this site.

### CWE

CWE-319

### CVSS2

AV:N/AC:M/Au:N/C:P/I:P/A:N

Access Vector	Network
Access Complexity	Medium
Authentication	None
Confidentiality	Partial
Integrity Impact	Partial
Availability Impact	None

### CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N

Base Score	5.4
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Unchanged
Confidentiality	Low
Integrity Impact	Low
Availability Impact	None

## Impact

Possible information disclosure.

<http://10.10.236.31/>

Verified

## Request

```
GET /openemr/public/assets/i18next/dist/umd/ HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 8595e182db21cbbc10c83c2c4cf193d3
Acunetix-Aspect-ScanID: 816589585389164376
Acunetix-Aspect-Queries: filelist;packages;aspectalerts;routes
Referer: http://10.10.236.31/openemr/public/assets/i18next/dist/umd/
Cookie: OpenEMR=Dj68HNoGw-vYWT2k81NHDiqIHhLtRgfoVY0Tqo%2Cj6JeJm5aU
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 10.10.236.31
Connection: Keep-alive
```

<http://192.168.145.128/>

Verified

## Request

```
GET /openemr/public/assets/ HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58adee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/public/assets/
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

## Recommendation

The site should send and receive data over a secure (HTTPS) connection.

# SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT

The organization establishes and manages cryptographic keys for required cryptography employed within the information system.

**No alerts in this category**

## SC-23 SESSION AUTHENTICITY

---

The information system protects the authenticity of communications sessions.

**No alerts in this category**

## SI-2 FLAW REMEDIATION

---

The organization identifies, reports, and corrects information system flaws, tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation, installs security-relevant software and firmware updates

### Vulnerable package dependencies [high]

---

One or more packages that are used in your web application are affected by known vulnerabilities. Please consult the details section for more information about each affected package.

**CWE**

CWE-1104

### Impact

---

The impact of this vulnerability is different for each vulnerable package. It's recommended to investigate each vulnerable package individually.

#### <http://10.10.236.31/openemr/>

List of vulnerable **composer** packages:

**Package:** dompdf/dompdf

**Version:** 1.2.2

**CVE:** CVE-2022-41343

**Title:** Files or Directories Accessible to External Parties

**Description:** registerFont in FontMetrics.php in Dompdf before 2.0.1 allows remote file inclusion because a URI validation failure does not halt font registration, as demonstrated by a @font-face rule.

**CVSS V2:**

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

**CWE:** CWE-552

**References:**

- <https://github.com/dompdf/dompdf/releases/tag/v2.0.1>
- <https://github.com/dompdf/dompdf/issues/2994>
- <https://github.com/dompdf/dompdf/pull/2995>
- <https://tantosec.com/blog/cve-2022-41343/>

**Package:** dompdf/dompdf

**Version:** 1.2.2

**CVE:** CVE-2023-23924

**Title:** Incorrect Authorization

**Description:** Dompdf is an HTML to PDF converter. The URI validation on dompdf 2.0.1 can be bypassed on SVG parsing by passing `<image>` tags with uppercase letters. This may lead to arbitrary object unserialize on PHP < 8, through the `phar` URL wrapper. An attacker can exploit the vulnerability to call arbitrary URL with arbitrary protocols, if they can provide a SVG file to dompdf. In PHP versions before 8.0.0, it leads to arbitrary unserialize, that will lead to the very least to an arbitrary file deletion and even remote code execution, depending on classes that are available.

**CVSS V2:**

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

**CWE:** CWE-863

**References:**

- <https://github.com/dompdf/dompdf/security/advisories/GHSA-3cw5-7cxw-v5qg>
- <https://github.com/dompdf/dompdf/releases/tag/v2.0.2>
- <https://github.com/dompdf/dompdf/commit/7558f07f693b2ac3266089f21051e6b78c6a0c85>

**Package:** dompdf/dompdf

**Version:** 1.2.2

**CVE:** CVE-2023-24813

**Title:** Interpretation Conflict

**Description:** Dompdf is an HTML to PDF converter written in php. Due to the difference in the attribute parser of Dompdf and php-svg-lib, an attacker can still call arbitrary URLs with arbitrary protocols. Dompdf parses the href attribute of `image` tags and respects `xlink:href` even if `href` is specified. However, php-svg-lib, which is later used to parse the svg file, parses the href attribute. Since `href` is respected if both `xlink:href` and `href` is specified, it's possible to bypass the protection on the Dompdf side by providing an empty `xlink:href` attribute. An attacker can exploit the vulnerability to call arbitrary URLs with arbitrary protocols if they provide an SVG file to the Dompdf. In PHP versions before 8.0.0, it leads to arbitrary unserialize, which will lead, at the very least, to arbitrary file deletion and might lead to remote code execution, depending on available classes. This vulnerability has been addressed in commit `95009ea98` which has been included in release version 2.0.3. Users are advised to upgrade. There are no known workarounds for this vulnerability.

**CVSS V2:**

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

**CWE:** CWE-436

**References:**

- <https://github.com/dompdf/dompdf/security/advisories/GHSA-56gj-mvh6-rp75>
- <https://github.com/dompdf/dompdf/commit/95009ea98230f9b084b040c34e3869ef3dccc9aa>

**Package:** guzzlehttp/guzzle

**Version:** 7.4.4

**CVE:** CVE-2022-31091

**Title:**

**Description:** Guzzle, an extensible PHP HTTP client. `Authorization` and `Cookie` headers on requests are sensitive information. In affected versions on making a request which responds with a redirect to a URI with a different port, if we choose to follow it, we should remove the `Authorization` and `Cookie` headers from the request, before continuing. Previously, we would only consider a change in host or scheme. Affected Guzzle 7 users should upgrade to Guzzle 7.4.5 as soon as possible. Affected users using any earlier series of Guzzle should upgrade to Guzzle 6.5.8 or 7.4.5. Note that a partial fix was implemented in Guzzle 7.4.2, where a change in host would trigger removal of the curl-added Authorization header, however this earlier fix did not cover change in scheme or change in port. An alternative approach would be to use your own redirect middleware, rather than ours, if you are unable to upgrade. If you do not require or expect redirects to be followed, one should simply disable redirects all together.

**CVSS V2:** AV:N/AC:L/Au:S/C:P/I:N/A:N

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N

**CWE:** NVD-CWE-noinfo

**References:**

- <https://github.com/guzzle/guzzle/commit/1dd98b0564cb3f6bd16ce683cb755f94c10fdb82>
- <https://github.com/guzzle/guzzle/security/advisories/GHSA-q559-8m2m-g699>
- <https://www.debian.org/security/2022/dsa-5246>

**Package:** guzzlehttp/guzzle

**Version:** 7.4.4

**CVE:** CVE-2022-31090

**Title:** Exposure of Sensitive Information to an Unauthorized Actor

**Description:** Guzzle, an extensible PHP HTTP client. `Authorization` headers on requests are sensitive information. In affected versions when using our Curl handler, it is possible to use the `CURLOPT\_HTTPAUTH` option to specify an `Authorization` header. On making a request which responds with a redirect to a URI with a different origin (change in host, scheme or port), if we choose to follow it, we should remove the `CURLOPT\_HTTPAUTH` option before continuing, stopping curl from appending the `Authorization` header to the new request. Affected Guzzle 7 users should upgrade to Guzzle 7.4.5 as soon as possible. Affected users using any earlier series of Guzzle should upgrade to Guzzle 6.5.8 or 7.4.5. Note that a partial fix was implemented in Guzzle 7.4.2, where a change in host would trigger removal of the curl-added Authorization header, however this earlier fix did not cover change in scheme or change in port. If you do not require or expect redirects to be followed, one should simply disable redirects all together. Alternatively, one can specify to use the Guzzle steam handler backend, rather than curl.

**CVSS V2:** AV:N/AC:L/Au:S/C:P/I:N/A:N

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N

**CWE:** CWE-200

**References:**

- <https://github.com/guzzle/guzzle/commit/1dd98b0564cb3f6bd16ce683cb755f94c10fdb82>
- <https://github.com/guzzle/guzzle/security/advisories/GHSA-25mq-v84q-4j7r>

- <https://www.debian.org/security/2022/dsa-5246>

**Package:** knplabs/knp-snappy

**Version:** 1.4.1

**CVE:** CVE-2023-28115

**Title:** Deserialization of Untrusted Data

**Description:** Snappy is a PHP library allowing thumbnail, snapshot or PDF generation from a url or a html page. Prior to version 1.4.2, Snappy is vulnerable to PHAR deserialization due to a lack of checking on the protocol before passing it into the `file\_exists()` function. If an attacker can upload files of any type to the server he can pass in the phar:// protocol to unserialize the uploaded file and instantiate arbitrary PHP objects. This can lead to remote code execution especially when snappy is used with frameworks with documented POP chains like Laravel/Symfony vulnerable developer code. If a user can control the output file from the `generateFromHtml()` function, it will invoke deserialization. This vulnerability is capable of remote code execution if Snappy is used with frameworks or developer code with vulnerable POP chains. It has been fixed in version 1.4.2.

**CVSS V2:**

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

**CWE:** CWE-502

**References:**

- <https://github.com/KnpLabs/snappy/releases/tag/v1.4.2>
- <https://github.com/KnpLabs/snappy/security/advisories/GHSA-gq6w-q6wh-jggc>
- <https://github.com/KnpLabs/snappy/commit/b66f79334421c26d9c244427963fa2d92980b5d3>
- <https://github.com/KnpLabs/snappy/commit/1ee6360cbdbea5d09705909a150df7963a88efd6>
- <https://github.com/KnpLabs/snappy/blob/5126fb5b335ec929a226314d40cd8dad497c3d67/src/Knp/Snappy/AbstractGenerator.php#L670>
- <https://github.com/KnpLabs/snappy/pull/469>

**Package:** phpseclib/phpseclib

**Version:** 2.0.37

**CVE:** CVE-2023-27560

**Title:** Loop with Unreachable Exit Condition ('Infinite Loop')

**Description:** Math/PrimeField.php in phpseclib 3.x before 3.0.19 has an infinite loop with composite primefields.

**CVSS V2:**

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

**CWE:** CWE-835

**References:**

- <https://github.com/phpseclib/phpseclib/commit/6298d1cd55c3ffa44533bd41906caec246b60440>
- <https://github.com/phpseclib/phpseclib/releases/tag/3.0.19>

**Package:** smarty/smarty

**Version:** 2.6.33

**CVE:** CVE-2021-26119

**Title:**

**Description:** Smarty before 3.1.39 allows a Sandbox Escape because \$smarty.template\_object can be accessed in sandbox mode.

**CVSS V2:** AV:N/AC:L/Au:N/C:N/I:P/A:N

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

**CWE:** NVD-CWE-noinfo

**References:**

- <https://github.com/smarty-php/smarty/blob/master/CHANGELOG.md>
- <https://lists.debian.org/debian-lts-announce/2021/04/msg00004.html>
- <https://lists.debian.org/debian-lts-announce/2021/04/msg00014.html>
- <https://security.gentoo.org/glsa/202105-06>
- <https://www.debian.org/security/2022/dsa-5151>

**Package:** smarty/smarty

**Version:** 2.6.33

**CVE:** CVE-2021-26120

**Title:** Improper Control of Generation of Code ('Code Injection')

**Description:** Smarty before 3.1.39 allows code injection via an unexpected function name after a {function name= substring.

**CVSS V2:** AV:N/AC:L/Au:N/C:P/I:P/A:P

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

**CWE:** CWE-94

**References:**

- <https://github.com/smarty-php/smarty/blob/master/CHANGELOG.md>
- <https://lists.debian.org/debian-lts-announce/2021/04/msg00004.html>
- <https://lists.debian.org/debian-lts-announce/2021/04/msg00014.html>
- <https://security.gentoo.org/glsa/202105-06>
- <https://www.debian.org/security/2022/dsa-5151>

**Package:** smarty/smarty

**Version:** 2.6.33

**CVE:** CVE-2017-1000480

**Title:** Improper Control of Generation of Code ('Code Injection')

**Description:** Smarty 3 before 3.1.32 is vulnerable to a PHP code injection when calling fetch() or display() functions on custom resources that does not sanitize template name.

**CVSS V2:** AV:N/AC:L/Au:N/C:P/I:P/A:P

**CVSS V3:** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

**CWE:** CWE-94

**References:**

- [https://github.com/smarty-php/smarty/blob/master/change\\_log.txt](https://github.com/smarty-php/smarty/blob/master/change_log.txt)
- <https://www.debian.org/security/2018/dsa-4094>
- <https://lists.debian.org/debian-lts-announce/2018/02/msg00000.html>
- <https://lists.debian.org/debian-lts-announce/2018/01/msg00023.html>

**Package:** smarty/smarty

**Version:** 2.6.33

**CVE:** CVE-2018-13982

**Title:** Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

**Description:** Smarty\_Security::isTrustedResourceDir() in Smarty before 3.1.33 is prone to a path traversal vulnerability due to insufficient template code sanitization. This allows attackers controlling the executed template code to bypass the trusted directory security restriction and read arbitrary files.

**CVSS V2:** AV:N/AC:L/Au:N/C:P/I:N/A:N

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

**CWE:** CWE-22

**References:**

- <https://github.com/smarty-php/smarty/commit/f9ca3c63d1250bb56b2bda609dcc9dd81f0065f8>
- <https://github.com/smarty-php/smarty/commit/c9dbe1d08c081912d02bd851d1d1b6388f6133d1>
- <https://github.com/smarty-php/smarty/commit/bcedfd6b58bed4a7366336979ebaa5a240581531>
- <https://github.com/smarty-php/smarty/commit/8d21f38dc35c4cd6b31c2f23fc9b8e5adbc56fe>
- <https://github.com/smarty-php/smarty/commit/2e081a51b1effddb23f87952959139ac62654d50>
- [https://github.com/sbaresearch/advisories/tree/public/2018/SBA-ADV-20180420-01\\_Smarty\\_Path\\_Traversal](https://github.com/sbaresearch/advisories/tree/public/2018/SBA-ADV-20180420-01_Smarty_Path_Traversal)
- <https://lists.debian.org/debian-lts-announce/2021/04/msg00004.html>
- <https://lists.debian.org/debian-lts-announce/2021/04/msg00014.html>
- <https://lists.debian.org/debian-lts-announce/2021/10/msg00015.html>

**Package:** smarty/smarty

**Version:** 2.6.33

**CVE:** CVE-2021-21408

**Title:** Improper Input Validation

**Description:** Smarty is a template engine for PHP, facilitating the separation of presentation (HTML/CSS) from application logic. Prior to versions 3.1.43 and 4.0.3, template authors could run restricted static php methods. Users should upgrade to version 3.1.43 or 4.0.3 to receive a patch.

**CVSS V2:** AV:N/AC:L/Au:S/C:P/I:P/A:P

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

**CWE:** CWE-20

**References:**

- <https://github.com/smarty-php/smarty/commit/19ae410bf56007a5ef24441cdc6414619cfaf664>
- <https://github.com/smarty-php/smarty/releases/tag/v3.1.43>
- <https://github.com/smarty-php/smarty/security/advisories/GHSA-4h9c-v5vg-5m6m>
- <https://github.com/smarty-php/smarty/releases/tag/v4.0.3>
- <https://lists.debian.org/debian-lts-announce/2022/05/msg00005.html>
- <https://www.debian.org/security/2022/dsa-5151>
- <https://security.gentoo.org/glsa/202209-09>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/L777JIBIWJV34HS7LXPIDWASG7TT4LNI/>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/BRAJVDRGCIY5UZ2PQHKDTT7RMKG6WJQQ/>

**Package:** smarty/smarty

**Version:** 2.6.33

**CVE:** CVE-2021-29454

**Title:** Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')

**Description:** Smarty is a template engine for PHP, facilitating the separation of presentation (HTML/CSS) from application logic. Prior to versions 3.1.42 and 4.0.2, template authors could run arbitrary PHP code by crafting a malicious math string. If a math string was passed through as user provided data to the math function, external users could run arbitrary PHP code by crafting a malicious math string. Users should upgrade to version 3.1.42 or 4.0.2 to receive a patch.

**CVSS V2:** AV:N/AC:L/Au:S/C:P/I:P/A:P

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

**CWE:** CWE-74

**References:**

- <https://github.com/smarty-php/smarty/commit/215d81a9fa3cd63d82fb3ab56ecaf97cf1e7db71>
- <https://github.com/smarty-php/smarty/security/advisories/GHSA-29gp-2c3m-3j6m>
- <https://packagist.org/packages/smarty/smarty>
- <https://github.com/smarty-php/smarty/releases/tag/v3.1.42>
- <https://www.smarty.net/docs/en/language.function.math.tpl>
- <https://github.com/smarty-php/smarty/releases/tag/v4.0.2>
- <https://lists.debian.org/debian-lts-announce/2022/05/msg00005.html>
- <https://www.debian.org/security/2022/dsa-5151>
- <https://security.gentoo.org/glsa/202209-09>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/L777JIBIWJV34HS7LXPIDWASG7TT4LNI/>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/BRAJVDRGCIY5UZ2PQHKDTT7RMKG6WJQQ/>

**Package:** smarty/smarty

**Version:** 2.6.33

**CVE:** CVE-2022-29221

**Title:** Improper Control of Generation of Code ('Code Injection')

**Description:** Smarty is a template engine for PHP, facilitating the separation of presentation (HTML/CSS) from application logic. Prior to versions 3.1.45 and 4.1.1, template authors could inject php code by choosing a malicious {block} name or {include} file name. Sites that cannot fully trust template authors should upgrade to versions 3.1.45 or 4.1.1 to receive a patch for this issue. There are currently no known workarounds.

**CVSS V2:** AV:N/AC:L/Au:S/C:P/I:P/A:P

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

**CWE:** CWE-94

**References:**

- <https://github.com/smarty-php/smarty/releases/tag/v3.1.45>
- <https://github.com/smarty-php/smarty/security/advisories/GHSA-634x-pc3q-cf4c>
- <https://github.com/smarty-php/smarty/commit/64ad6442ca1da31cefdb5c9874262b702ccddd>
- <https://github.com/smarty-php/smarty/releases/tag/v4.1.1>
- <https://www.debian.org/security/2022/dsa-5151>
- <https://lists.debian.org/debian-lts-announce/2022/05/msg00044.html>
- <https://security.gentoo.org/glsa/202209-09>

- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/L777JIBIWJV34HS7LXPIDWASG7TT4LNI/>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/BRAJVDRGCIY5UZ2PQHKDTT7RMKG6WJQQ/>

**Package:** twig/twig

**Version:** 3.4.1

**CVE:** CVE-2022-39261

**Title:** Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

**Description:** Twig is a template language for PHP. Versions 1.x prior to 1.44.7, 2.x prior to 2.15.3, and 3.x prior to 3.4.3 encounter an issue when the filesystem loader loads templates for which the name is a user input. It is possible to use the `source` or `include` statement to read arbitrary files from outside the templates' directory when using a namespace like `@somewhere/..//some.file`. In such a case, validation is bypassed. Versions 1.44.7, 2.15.3, and 3.4.3 contain a fix for validation of such template names. There are no known workarounds aside from upgrading.

**CVSS V2:**

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

**CWE:** CWE-22

**References:**

- <https://github.com/twigphp/Twig/commit/35f3035c5deb0041da7b84daf02dea074ddc7a0b>
- <https://github.com/twigphp/Twig/security/advisories/GHSA-52m2-vc4m-jj33>
- <https://www.drupal.org/sa-core-2022-016>
- <https://www.debian.org/security/2022/dsa-5248>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/2OKRUHPVLIQVFPPJ2UWC3WV3WQO763NR/>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/AUVTXMNPSZAHS3DWZEM56V5W4NPVR6L7/>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/NWRFPZSR74SYVJKBTKTMYUK36IJ3SQJP/>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/YU4ZYX62H2NUAKKGUES4RZIM4KMTKZ7F/>
- <https://lists.debian.org/debian-lts-announce/2022/10/msg00016.html>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/TW53TFJ6WWNXMUHOFACKATJTS7NIHVQE/>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/WV5TNNJLGG536TJH6DLCIAAZZIPV2GUD/>

## <http://192.168.145.128/openemr/>

List of vulnerable **composer** packages:

**Package:** dompdf/dompdf

**Version:** 1.2.2

**CVE:** CVE-2022-41343

**Title:** Files or Directories Accessible to External Parties

**Description:** registerFont in FontMetrics.php in Dompdf before 2.0.1 allows remote file inclusion because a URI validation failure does not halt font registration, as demonstrated by a @font-face rule.

**CVSS V2:**

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

**CWE:** CWE-552

**References:**

- <https://github.com/dompdf/dompdf/releases/tag/v2.0.1>
- <https://github.com/dompdf/dompdf/issues/2994>
- <https://github.com/dompdf/dompdf/pull/2995>
- <https://tantosec.com/blog/cve-2022-41343/>

**Package:** dompdf/dompdf

**Version:** 1.2.2

**CVE:** CVE-2023-23924

**Title:** Incorrect Authorization

**Description:** Dompdf is an HTML to PDF converter. The URI validation on dompdf 2.0.1 can be bypassed on SVG parsing by passing `<image>` tags with uppercase letters. This may lead to arbitrary object unserialize on PHP < 8, through the `phar` URL wrapper. An attacker can exploit the vulnerability to call arbitrary URL with arbitrary protocols, if they can provide a SVG file to dompdf. In PHP versions before 8.0.0, it leads to arbitrary unserialize, that will lead to the very least to an arbitrary file deletion and even remote code execution, depending on classes that are available.

**CVSS V2:**

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

**CWE:** CWE-863

**References:**

- <https://github.com/dompdf/dompdf/security/advisories/GHSA-3cw5-7cxw-v5qg>
- <https://github.com/dompdf/dompdf/releases/tag/v2.0.2>
- <https://github.com/dompdf/dompdf/commit/7558f07f693b2ac3266089f21051e6b78c6a0c85>

**Package:** dompdf/dompdf

**Version:** 1.2.2

**CVE:** CVE-2023-24813

**Title:** Interpretation Conflict

**Description:** Dompdf is an HTML to PDF converter written in php. Due to the difference in the attribute parser of Dompdf and php-svg-lib, an attacker can still call arbitrary URLs with arbitrary protocols. Dompdf parses the href attribute of `image` tags and respects `xlink:href` even if `href` is specified. However, php-svg-lib, which is later used to parse the svg file, parses the href attribute. Since `href` is respected if both `xlink:href` and `href` is specified, it's possible to bypass the protection on the Dompdf side by providing an empty `xlink:href` attribute. An attacker can exploit the vulnerability to call arbitrary URLs with arbitrary protocols if they provide an SVG file to the Dompdf. In PHP versions before 8.0.0, it leads to arbitrary unserialize, which will lead, at the very least, to arbitrary file deletion and might lead to remote code execution, depending on available classes. This vulnerability has been addressed in commit `95009ea98` which has been included in release version 2.0.3. Users are advised to upgrade. There are no known workarounds for this vulnerability.

**CVSS V2:**

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

**CWE:** CWE-436

**References:**

- <https://github.com/dompdf/dompdf/security/advisories/GHSA-56gj-mvh6-rp75>
- <https://github.com/dompdf/dompdf/commit/95009ea98230f9b084b040c34e3869ef3dccc9aa>

**Package:** guzzlehttp/guzzle

**Version:** 7.4.4

**CVE:** CVE-2022-31091

**Title:**

**Description:** Guzzle, an extensible PHP HTTP client. `Authorization` and `Cookie` headers on requests are sensitive information. In affected versions on making a request which responds with a redirect to a URI with a different port, if we choose to follow it, we should remove the `Authorization` and `Cookie` headers from the request, before containing. Previously, we would only consider a change in host or scheme. Affected Guzzle 7 users should upgrade to Guzzle 7.4.5 as soon as possible. Affected users using any earlier series of Guzzle should upgrade to Guzzle 6.5.8 or 7.4.5. Note that a partial fix was implemented in Guzzle 7.4.2, where a change in host would trigger removal of the curl-added Authorization header, however this earlier fix did not cover change in scheme or change in port. An alternative approach would be to use your own redirect middleware, rather than ours, if you are unable to upgrade. If you do not require or expect redirects to be followed, one should simply disable redirects all together.

**CVSS V2:** AV:N/AC:L/Au:S/C:P/I:N/A:N

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

**CWE:** NVD-CWE-noinfo

**References:**

- <https://github.com/guzzle/guzzle/commit/1dd98b0564cb3f6bd16ce683cb755f94c10fdbd82>
- <https://github.com/guzzle/guzzle/security/advisories/GHSA-q559-8m2m-g699>
- <https://www.debian.org/security/2022/dsa-5246>

**Package:** guzzlehttp/guzzle

**Version:** 7.4.4

**CVE:** CVE-2022-31090

**Title:** Exposure of Sensitive Information to an Unauthorized Actor

**Description:** Guzzle, an extensible PHP HTTP client. `Authorization` headers on requests are sensitive information. In affected versions when using our Curl handler, it is possible to use the `CURLOPT\_HTTPAUTH` option to specify an `Authorization` header. On making a request which responds with a redirect to a URI with a different origin (change in host, scheme or port), if we choose to follow it, we should remove the `CURLOPT\_HTTPAUTH` option before continuing, stopping curl from appending the `Authorization` header to the new request. Affected Guzzle 7 users should upgrade to Guzzle 7.4.5 as soon as possible. Affected users using any earlier series of Guzzle should upgrade to Guzzle 6.5.8 or 7.4.5. Note that a partial fix was implemented in Guzzle 7.4.2, where a change in host would trigger removal of the curl-added Authorization header, however this earlier fix did not cover change in scheme or change in port. If you do not require or expect redirects to be followed, one should simply disable redirects all together. Alternatively, one can specify to use the Guzzle steam handler backend, rather than curl.

**CVSS V2:** AV:N/AC:L/Au:S/C:P/I:N/A:N

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

**CWE:** CWE-200

**References:**

- <https://github.com/guzzle/guzzle/commit/1dd98b0564cb3f6bd16ce683cb755f94c10fdb82>
- <https://github.com/guzzle/guzzle/security/advisories/GHSA-25mq-v84q-4j7r>
- <https://www.debian.org/security/2022/dsa-5246>

**Package:** knplabs/knp-snappy

**Version:** 1.4.1

**CVE:** CVE-2023-28115

**Title:** Deserialization of Untrusted Data

**Description:** Snappy is a PHP library allowing thumbnail, snapshot or PDF generation from a url or a html page. Prior to version 1.4.2, Snappy is vulnerable to PHAR deserialization due to a lack of checking on the protocol before passing it into the `file\_exists()` function. If an attacker can upload files of any type to the server he can pass in the phar:// protocol to unserialize the uploaded file and instantiate arbitrary PHP objects. This can lead to remote code execution especially when snappy is used with frameworks with documented POP chains like Laravel/Symfony vulnerable developer code. If a user can control the output file from the `generateFromHtml()` function, it will invoke deserialization. This vulnerability is capable of remote code execution if Snappy is used with frameworks or developer code with vulnerable POP chains. It has been fixed in version 1.4.2.

**CVSS V2:**

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

**CWE:** CWE-502

**References:**

- <https://github.com/KnpLabs/snappy/releases/tag/v1.4.2>
- <https://github.com/KnpLabs/snappy/security/advisories/GHSA-gq6w-q6wh-jggc>
- <https://github.com/KnpLabs/snappy/commit/b66f79334421c26d9c244427963fa2d92980b5d3>
- <https://github.com/KnpLabs/snappy/commit/1ee6360cbdbea5d09705909a150df7963a88efd6>
- <https://github.com/KnpLabs/snappy/blob/5126fb5b335ec929a226314d40cd8dad497c3d67/src/Knp/Snappy/AbstractGenerator.php#L670>

- <https://github.com/KnpLabs/snappy/pull/469>

**Package:** phpseclib/phpseclib

**Version:** 2.0.37

**CVE:** CVE-2023-27560

**Title:** Loop with Unreachable Exit Condition ('Infinite Loop')

**Description:** Math/PrimeField.php in phpseclib 3.x before 3.0.19 has an infinite loop with composite primefields.

**CVSS V2:**

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

**CWE:** CWE-835

**References:**

- <https://github.com/phpseclib/phpseclib/commit/6298d1cd55c3ffa44533bd41906caec246b60440>
- <https://github.com/phpseclib/phpseclib/releases/tag/3.0.19>

**Package:** smarty/smarty

**Version:** 2.6.33

**CVE:** CVE-2021-26119

**Title:**

**Description:** Smarty before 3.1.39 allows a Sandbox Escape because \$smarty.template\_object can be accessed in sandbox mode.

**CVSS V2:** AV:N/AC:L/Au:N/C:N/I:P/A:N

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

**CWE:** NVD-CWE-noinfo

**References:**

- <https://github.com/smarty-php/smarty/blob/master/CHANGELOG.md>
- <https://lists.debian.org/debian-lts-announce/2021/04/msg00004.html>
- <https://lists.debian.org/debian-lts-announce/2021/04/msg00014.html>
- <https://security.gentoo.org/glsa/202105-06>
- <https://www.debian.org/security/2022/dsa-5151>

**Package:** smarty/smarty

**Version:** 2.6.33

**CVE:** CVE-2021-26120

**Title:** Improper Control of Generation of Code ('Code Injection')

**Description:** Smarty before 3.1.39 allows code injection via an unexpected function name after a {function name= substring.

**CVSS V2:** AV:N/AC:L/Au:N/C:P/I:P/A:P

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

**CWE:** CWE-94

**References:**

- <https://github.com/smarty-php/smarty/blob/master/CHANGELOG.md>
- <https://lists.debian.org/debian-lts-announce/2021/04/msg00004.html>
- <https://lists.debian.org/debian-lts-announce/2021/04/msg00014.html>
- <https://security.gentoo.org/glsa/202105-06>
- <https://www.debian.org/security/2022/dsa-5151>

**Package:** smarty/smarty

**Version:** 2.6.33

**CVE:** CVE-2017-1000480

**Title:** Improper Control of Generation of Code ('Code Injection')

**Description:** Smarty 3 before 3.1.32 is vulnerable to a PHP code injection when calling fetch() or display() functions on custom resources that does not sanitize template name.

**CVSS V2:** AV:N/AC:L/Au:N/C:P/I:P/A:P

**CVSS V3:** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

**CWE:** CWE-94

**References:**

- [https://github.com/smarty-php/smarty/blob/master/change\\_log.txt](https://github.com/smarty-php/smarty/blob/master/change_log.txt)
- <https://www.debian.org/security/2018/dsa-4094>

- <https://lists.debian.org/debian-lts-announce/2018/02/msg00000.html>
- <https://lists.debian.org/debian-lts-announce/2018/01/msg00023.html>

**Package:** smarty/smarty

**Version:** 2.6.33

**CVE:** CVE-2018-13982

**Title:** Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

**Description:** Smarty\_Security::isTrustedResourceDir() in Smarty before 3.1.33 is prone to a path traversal vulnerability due to insufficient template code sanitization. This allows attackers controlling the executed template code to bypass the trusted directory security restriction and read arbitrary files.

**CVSS V2:** AV:N/AC:L/Au:N/C:P/I:N/A:N

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

**CWE:** CWE-22

**References:**

- <https://github.com/smarty-php/smarty/commit/f9ca3c63d1250bb56b2bda609dcc9dd81f0065f8>
- <https://github.com/smarty-php/smarty/commit/c9dbe1d08c081912d02bd851d1d1b6388f6133d1>
- <https://github.com/smarty-php/smarty/commit/bcedfd6b58bed4a7366336979ebaa5a240581531>
- <https://github.com/smarty-php/smarty/commit/8d21f38dc35c4cd6b31c2f23fc9b8e5adbc56dfe>
- <https://github.com/smarty-php/smarty/commit/2e081a51b1effddb23f87952959139ac62654d50>
- [https://github.com/sbaresearch/advisories/tree/public/2018/SBA-ADV-20180420-01\\_Smarty\\_Path\\_Traversal](https://github.com/sbaresearch/advisories/tree/public/2018/SBA-ADV-20180420-01_Smarty_Path_Traversal)
- <https://lists.debian.org/debian-lts-announce/2021/04/msg00004.html>
- <https://lists.debian.org/debian-lts-announce/2021/04/msg00014.html>
- <https://lists.debian.org/debian-lts-announce/2021/10/msg00015.html>

**Package:** smarty/smarty

**Version:** 2.6.33

**CVE:** CVE-2021-21408

**Title:** Improper Input Validation

**Description:** Smarty is a template engine for PHP, facilitating the separation of presentation (HTML/CSS) from application logic. Prior to versions 3.1.43 and 4.0.3, template authors could run restricted static php methods. Users should upgrade to version 3.1.43 or 4.0.3 to receive a patch.

**CVSS V2:** AV:N/AC:L/Au:S/C:P/I:P/A:P

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

**CWE:** CWE-20

**References:**

- <https://github.com/smarty-php/smarty/commit/19ae410bf56007a5ef24441cdc6414619cfaf664>
- <https://github.com/smarty-php/smarty/releases/tag/v3.1.43>
- <https://github.com/smarty-php/smarty/security/advisories/GHSA-4h9c-v5vg-5m6m>
- <https://github.com/smarty-php/smarty/releases/tag/v4.0.3>
- <https://lists.debian.org/debian-lts-announce/2022/05/msg00005.html>
- <https://www.debian.org/security/2022/dsa-5151>
- <https://security.gentoo.org/glsa/202209-09>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/L777JIBIWJV34HS7LXPIDWASG7TT4LNI/>

- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/BRAJVDRGCIY5UZ2PQHKDTT7RMKG6WJQQ/>

**Package:** smarty/smarty

**Version:** 2.6.33

**CVE:** CVE-2021-29454

**Title:** Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')

**Description:** Smarty is a template engine for PHP, facilitating the separation of presentation (HTML/CSS) from application logic. Prior to versions 3.1.42 and 4.0.2, template authors could run arbitrary PHP code by crafting a malicious math string. If a math string was passed through as user provided data to the math function, external users could run arbitrary PHP code by crafting a malicious math string. Users should upgrade to version 3.1.42 or 4.0.2 to receive a patch.

**CVSS V2:** AV:N/AC:L/Au:S/C:P/I:P/A:P

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

**CWE:** CWE-74

**References:**

- <https://github.com/smarty-php/smarty/commit/215d81a9fa3cd63d82fb3ab56ecaf97cf1e7db71>
- <https://github.com/smarty-php/smarty/security/advisories/GHSA-29gp-2c3m-3j6m>
- <https://packagist.org/packages/smarty/smarty>
- <https://github.com/smarty-php/smarty/releases/tag/v3.1.42>
- <https://www.smarty.net/docs/en/language.function.math.tpl>
- <https://github.com/smarty-php/smarty/releases/tag/v4.0.2>
- <https://lists.debian.org/debian-lts-announce/2022/05/msg00005.html>
- <https://www.debian.org/security/2022/dsa-5151>
- <https://security.gentoo.org/glsa/202209-09>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/L777JIBIWJV34HS7LXPIDWASG7TT4LNI/>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/BRAJVDRGCIY5UZ2PQHKDTT7RMKG6WJQQ/>

**Package:** smarty/smarty

**Version:** 2.6.33

**CVE:** CVE-2022-29221

**Title:** Improper Control of Generation of Code ('Code Injection')

**Description:** Smarty is a template engine for PHP, facilitating the separation of presentation (HTML/CSS) from application logic. Prior to versions 3.1.45 and 4.1.1, template authors could inject php code by choosing a malicious {block} name or {include} file name. Sites that cannot fully trust template authors should upgrade to versions 3.1.45 or 4.1.1 to receive a patch for this issue. There are currently no known workarounds.

**CVSS V2:** AV:N/AC:L/Au:S/C:P/I:P/A:P

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

**CWE:** CWE-94

**References:**

- <https://github.com/smarty-php/smarty/releases/tag/v3.1.45>
- <https://github.com/smarty-php/smarty/security/advisories/GHSA-634x-pc3q-cf4c>
- <https://github.com/smarty-php/smarty/commit/64ad6442ca1da31cefdab5c9874262b702ccddd>

- <https://github.com/smarty-php/smarty/releases/tag/v4.1.1>
- <https://www.debian.org/security/2022/dsa-5151>
- <https://lists.debian.org/debian-lts-announce/2022/05/msg00044.html>
- <https://security.gentoo.org/glsa/202209-09>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/L777JIBIWJV34HS7LXPIDWASG7TT4LNI/>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/BRAJVDRGCIY5UZ2PQHKDTT7RMKG6WJQQ/>

**Package:** twig/twig

**Version:** 3.4.1

**CVE:** CVE-2022-39261

**Title:** Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

**Description:** Twig is a template language for PHP. Versions 1.x prior to 1.44.7, 2.x prior to 2.15.3, and 3.x prior to 3.4.3 encounter an issue when the filesystem loader loads templates for which the name is a user input. It is possible to use the `source` or `include` statement to read arbitrary files from outside the templates' directory when using a namespace like `@somewhere/..//some.file`. In such a case, validation is bypassed. Versions 1.44.7, 2.15.3, and 3.4.3 contain a fix for validation of such template names. There are no known workarounds aside from upgrading.

**CVSS V2:**

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

**CWE:** CWE-22

**References:**

- <https://github.com/twigphp/Twig/commit/35f3035c5deb0041da7b84daf02dea074ddc7a0b>
- <https://github.com/twigphp/Twig/security/advisories/GHSA-52m2-vc4m-jj33>
- <https://www.drupal.org/sa-core-2022-016>
- <https://www.debian.org/security/2022/dsa-5248>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/2OKRUHPVLIQVFPPJ2UWC3WV3WQO763NR/>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/AUVTXMNPSZAHS3DWZEM56V5W4NPVR6L7/>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/NWRFPZSR74SYVJKBTKTMYUK36IJ3SQJP/>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/YU4ZYX62H2NUAKKGUES4RZIM4KMTKZ7F/>
- <https://lists.debian.org/debian-lts-announce/2022/10/msg00016.html>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/TW53TFJ6WWNXMUHOFACKATJTS7NIHVQE/>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/WV5TNNJLGG536TJH6DLCIAAZZIPV2GUD/>

## Recommendation

---

It's recommended to update the vulnerable packages to the latest version (if a fix exists). If a fix does not exist, you may want to suggest changes that address the vulnerability to the package maintainer or remove the package from your dependency tree.

## Vulnerable package dependencies [medium]

---

One or more packages that are used in your web application are affected by known vulnerabilities. Please consult the details section for more information about each affected package.

### CWE

CWE-1104

## Impact

---

The impact of this vulnerability is different for each vulnerable package. It's recommended to investigate each vulnerable package individually.

### <http://10.10.236.31/openemr/>

List of vulnerable **composer** packages:

**Package:** dompdf/dompdf

**Version:** 1.2.2

**CVE:** CVE-2022-0085

**Title:** Server-Side Request Forgery (SSRF)

**Description:** Server-Side Request Forgery (SSRF) in GitHub repository dompdf/dompdf prior to 2.0.0.

**CVSS V2:** AV:N/AC:M/Au:N/C:N/I:P/A:N

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

**CWE:** CWE-918

**References:**

- <https://github.com/dompdf/dompdf/commit/bb1ef65011a14730b7cfbe73506b4bb8a03704bd>
- <https://huntr.dev/bounties/73dbcc78-5ba9-492f-9133-13bbc9f31236>

**Package:** dompdf/dompdf

**Version:** 1.2.2

**CVE:** CVE-2022-2400

**Title:** External Control of File Name or Path

**Description:** External Control of File Name or Path in GitHub repository dompdf/dompdf prior to 2.0.0.

**CVSS V2:**

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

**CWE:** CWE-73

**References:**

- <https://huntr.dev/bounties/a6da5e5e-86be-499a-a3c3-2950f749202a>
- <https://github.com/dompdf/dompdf/commit/99aeec1efec9213e87098d42eb09439e7ee0bb6a>

**Package:** smarty/smarty

**Version:** 2.6.33

**CVE:** CVE-2018-16831

**Title:** Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

**Description:** Smarty before 3.1.33-dev-4 allows attackers to bypass the trusted\_dir protection mechanism via a file:../ substring in an include statement.

**CVSS V2:** AV:N/AC:M/Au:N/C:C/I:N/A:N

**CVSS V3:** CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N

**CWE:** CWE-22

**References:**

- <https://github.com/smarty-php/smarty/issues/486>

**Package:** smarty/smarty

**Version:** 2.6.33

**CVE:** CVE-2018-25047

**Title:** Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

**Description:** In Smarty before 3.1.47 and 4.x before 4.2.1, libs/plugins/function.mailto.php allows XSS. A web page that uses smarty\_function\_mailto, and that could be parameterized using GET or POST input parameters, could allow injection of JavaScript code by a user.

**CVSS V2:**

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N

**CWE:** CWE-79

**References:**

- <https://github.com/smarty-php/smarty/releases/tag/v4.2.1>
- <https://github.com/smarty-php/smarty/releases/tag/v3.1.47>
- <https://bugs.gentoo.org/870100>
- <https://github.com/smarty-php/smarty/issues/454>
- <https://security.gentoo.org/glsa/202209-09>
- <https://lists.debian.org/debian-lts-announce/2023/01/msg00002.html>

**Package:** smarty/smarty

**Version:** 2.6.33

**CVE:** CVE-2023-28447

**Title:** Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

**Description:** Smarty is a template engine for PHP. In affected versions smarty did not properly escape javascript code. An attacker could exploit this vulnerability to execute arbitrary JavaScript code in the context of the user's browser session. This may lead to unauthorized access to sensitive user data, manipulation of the web application's behavior, or unauthorized actions performed on behalf of the user. Users are advised to upgrade to either version 3.1.48 or to 4.3.1 to resolve this issue. There are no known workarounds for this vulnerability.

**CVSS V2:**

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

**CWE:** CWE-79

**References:**

- <https://github.com/smarty-php/smarty/security/advisories/GHSA-7j98-h7fp-4vwj>
- <https://github.com/smarty-php/smarty/commit/685662466f653597428966d75a661073104d713d>

## <http://192.168.145.128/openemr/>

List of vulnerable **composer** packages:

**Package:** dompdf/dompdf

**Version:** 1.2.2

**CVE:** CVE-2022-0085

**Title:** Server-Side Request Forgery (SSRF)

**Description:** Server-Side Request Forgery (SSRF) in GitHub repository dompdf/dompdf prior to 2.0.0.

**CVSS V2:** AV:N/AC:M/Au:N/C:N/I:P/A:N

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

**CWE:** CWE-918

**References:**

- <https://github.com/dompdf/dompdf/commit/bb1ef65011a14730b7cfbe73506b4bb8a03704bd>
- <https://huntr.dev/bounties/73dbcc78-5ba9-492f-9133-13bbc9f31236>

**Package:** dompdf/dompdf

**Version:** 1.2.2

**CVE:** CVE-2022-2400

**Title:** External Control of File Name or Path

**Description:** External Control of File Name or Path in GitHub repository dompdf/dompdf prior to 2.0.0.

**CVSS V2:**

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

**CWE:** CWE-73

**References:**

- <https://huntr.dev/bounties/a6da5e5e-86be-499a-a3c3-2950f749202a>
- <https://github.com/dompdf/dompdf/commit/99aeec1efec9213e87098d42eb09439e7ee0bb6a>

**Package:** smarty/smarty

**Version:** 2.6.33

**CVE:** CVE-2018-16831

**Title:** Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

**Description:** Smarty before 3.1.33-dev-4 allows attackers to bypass the trusted\_dir protection mechanism via a file:../../ substring in an include statement.

**CVSS V2:** AV:N/AC:M/Au:N/C:C/I:N/A:N

**CVSS V3:** CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N

**CWE:** CWE-22

**References:**

- <https://github.com/smarty-php/smarty/issues/486>

**Package:** smarty/smarty

**Version:** 2.6.33

**CVE:** CVE-2018-25047

**Title:** Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

**Description:** In Smarty before 3.1.47 and 4.x before 4.2.1, libs/plugins/function.mailto.php allows XSS. A web page that uses smarty\_function\_mailto, and that could be parameterized using GET or POST input parameters, could allow injection of JavaScript code by a user.

**CVSS V2:**

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N

**CWE:** CWE-79

**References:**

- <https://github.com/smarty-php/smarty/releases/tag/v4.2.1>
- <https://github.com/smarty-php/smarty/releases/tag/v3.1.47>
- <https://bugs.gentoo.org/870100>
- <https://github.com/smarty-php/smarty/issues/454>
- <https://security.gentoo.org/glsa/202209-09>
- <https://lists.debian.org/debian-lts-announce/2023/01/msg00002.html>

**Package:** smarty/smarty

**Version:** 2.6.33

**CVE:** CVE-2023-28447

**Title:** Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

**Description:** Smarty is a template engine for PHP. In affected versions smarty did not properly escape javascript code. An attacker could exploit this vulnerability to execute arbitrary JavaScript code in the context of the user's browser session. This may lead to unauthorized access to sensitive user data, manipulation of the web application's behavior, or unauthorized actions performed on behalf of the user. Users are advised to upgrade to either version 3.1.48 or to 4.3.1 to resolve this issue. There are no known workarounds for this vulnerability.

**CVSS V2:**

**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

**CWE:** CWE-79

**References:**

- <https://github.com/smarty-php/smarty/security/advisories/GHSA-7j98-h7fp-4vwj>
- <https://github.com/smarty-php/smarty/commit/685662466f653597428966d75a661073104d713d>

## Recommendation

It's recommended to update the vulnerable packages to the latest version (if a fix exists). If a fix does not exist, you may want to suggest changes that address the vulnerability to the package maintainer or

remove the package from your dependency tree.

## Vulnerable JavaScript libraries

---

You are using one or more vulnerable JavaScript libraries. One or more vulnerabilities were reported for this version of the library. Consult Attack details and Web References for more information about the affected library and the vulnerabilities that were reported.

### CWE

CWE-937

### CVSS2

AV:N/AC:L/Au:N/C:P/I:P/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	Partial
Availability Impact	None

### CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N

Base Score	6.5
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	Low
Availability Impact	None

## Impact

---

Consult References for more information.

<http://10.10.236.31/>

Confidence: 95%

- **jQuery 1.10.2**

- URL: <http://10.10.236.31/openemr/public/assets/jquery-datetimepicker/>
- Detection method: The library's name and version were determined based on its dynamic behavior.
- CVE-ID: CVE-2015-9251, CVE-2020-11022, CVE-2020-11023
- Description: Possible Cross Site Scripting via third-party text/javascript responses / In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. / In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing option elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.
- References:

- <https://github.com/jquery/jquery/issues/2432>
- <http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/>
- <https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/>
- <https://mksben.lo.cm/2020/05/jquery3.5.0-xss.html>
- <https://jquery.com/upgrade-guide/3.5/>
- <https://api.jquery.com/jQuery.htmlPrefilter/>
- <https://www.cvedetails.com/cve/CVE-2020-11022/>
- <https://github.com/advisories/GHSA-gxr4-xjj5-5px2>
- <https://www.cvedetails.com/cve/CVE-2020-11023/>
- <https://github.com/advisories/GHSA-jpcq-cgw6-v4j6>

## Request

---

```
GET /openemr/public/assets/jquery-datetimepicker/ HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 8595e182db21cbbc10c83c2c4cf193d3
Acunetix-Aspect-ScanID: 816589585389164376
Acunetix-Aspect-Queries: filelist;packages;aspectalerts;routes
Referer: http://10.10.236.31/openemr/public/assets/jquery-datetimepicker/
Cookie: OpenEMR=Dj68HNoGw-vYWT2k81NHDiqIHhLtRgfoVY0Tqo%2Cj6JeJm5aU
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 10.10.236.31
Connection: Keep-alive
```

## <http://10.10.236.31/>

Verified

- **jQuery UI 1.12.1**

- URL: <http://10.10.236.31/openemr/public/assets/jquery-ui/jquery-ui.js>
- Detection method: The library's name and version were determined based on the file's syntax fingerprint, and contents. Acunetix verified the library version and the associated vulnerabilities with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- CVE-ID: CVE-2021-41184
- Description: XSS in the 'of' option of the '.position()' util
- References:
  - <https://blog.jqueryui.com/2021/10/jquery-ui-1-13-0-released/>
  - <https://github.com/jquery/jquery-ui/security/advisories/GHSA-gpqq-952q-5327>

## Request

---

```
GET /openemr/public/assets/jquery-ui/jquery-ui.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 8595e182db21cbbc10c83c2c4cf193d3
Acunetix-Aspect-ScanID: 816589585389164376
Acunetix-Aspect-Queries: aspectalerts;routes
```

Referer: http://10.10.236.31/openemr/Documentation/help\_files/openemr\_installation\_help.php  
Cookie: OpenEMR=b3DHM9s5BR72IjC3y6GcpBb736abtMj3%2CfzaSNeoS-j94pMx  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
Accept-Encoding: gzip,deflate,br  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)  
Chrome/109.0.0.0 Safari/537.36  
Host: 10.10.236.31  
Connection: Keep-alive

**http://10.10.236.31/**

Confidence: 95%

- **jQuery UI Datepicker 1.12.1**

- URL: http://10.10.236.31/openemr/public/assets/jquery-ui/jquery-ui.js
- Detection method: The library's name and version were determined based on the file's contents.
- CVE-ID: CVE-2021-41182, CVE-2021-41183
- Description: XSS in the 'altField' option of the Datepicker widget / XSS in '\*Text' options of the Datepicker widget
- References:
  - https://blog.jqueryui.com/2021/10/jquery-ui-1-13-0-released/
  - https://github.com/jquery/jquery-ui/security/advisories/GHSA-9gj3-hwp5-pmwv
  - https://github.com/jquery/jquery-ui/security/advisories/GHSA-j7qv-pgf6-hvh4

## Request

GET /openemr/public/assets/jquery-ui/jquery-ui.js HTTP/1.1  
Acunetix-Aspect: enabled  
Acunetix-Aspect-Password: 8595e182db21cbbc10c83c2c4cf193d3  
Acunetix-Aspect-ScanID: 816589585389164376  
Acunetix-Aspect-Queries: aspectalerts;routes  
Referer: http://10.10.236.31/openemr/Documentation/help\_files/openemr\_installation\_help.php  
Cookie: OpenEMR=b3DHM9s5BR72IjC3y6GcpBb736abtMj3%2CfzaSNeoS-j94pMx  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
Accept-Encoding: gzip,deflate,br  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)  
Chrome/109.0.0.0 Safari/537.36  
Host: 10.10.236.31  
Connection: Keep-alive

**http://10.10.236.31/**

Verified

- **jQuery 1.12.4**

- URL: http://10.10.236.31/openemr/public/assets/jquery-ui/external/jquery/jquery.js
- Detection method: The library's name and version were determined based on the file's syntax fingerprint, and contents. Acunetix verified the library version and the associated vulnerabilities with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.

- CVE-ID: CVE-2015-9251, CVE-2020-11022, CVE-2020-11023
- Description: Possible Cross Site Scripting via third-party text/javascript responses (1.12.0-1.12.2 mitigation reverted) / In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. / In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing option elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.
- References:
  - <https://github.com/jquery/jquery/issues/2432>
  - <https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/>
  - <https://mksben.lo.cm/2020/05/jquery3.5.0-xss.html>
  - <https://jquery.com/upgrade-guide/3.5/>
  - <https://api.jquery.com/jQuery.htmlPrefilter/>
  - <https://www.cvedetails.com/cve/CVE-2020-11022/>
  - <https://github.com/advisories/GHSA-gxr4-xjj5-5px2>
  - <https://www.cvedetails.com/cve/CVE-2020-11023/>
  - <https://github.com/advisories/GHSA-jpcq-cgw6-v4j6>

## Request

---

```
GET /openemr/public/assets/jquery-ui/external/jquery/jquery.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 8595e182db21cbbc10c83c2c4cf193d3
Acunetix-Aspect-ScanID: 816589585389164376
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://10.10.236.31/openemr/public/assets/jquery-ui/
Cookie: OpenEMR=b3DHM9s5BR72IjC3y6GcpBb736abtMj3%2CfzaSNeoS-j94pMx
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 10.10.236.31
Connection: Keep-alive
```

**http://192.168.145.128/**

Confidence: 95%

- **AngularJS 1.4.8**

- URL: <https://cdnjs.cloudflare.com/ajax/libs/angular.js/1.4.8/angular.js>
- Detection method: The library's name and version were determined based on the file's CDN URI.
- CVE-ID: CVE-2020-7676
- Description: Prototype pollution / Cross-Site Scripting.
- References:
  - <https://github.com/angular/angular.js/commit/726f49dcf6c23106ddaf5cf5e2e592841db743a>
  - <https://github.com/angular/angular.js/blob/master/CHANGELOG.md#179-pollution-eradication-2019-11-19>

- <https://nvd.nist.gov/vuln/detail/CVE-2020-7676>

## Request

---

```
GET /openemr/public/assets/checklist-model/ HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/public/assets/
Cookie: OpenEMR=g3GhfkD5xIsb3Ge5m8KYxfe43LFtvIbo%2CVxmCKL9iQGY052L
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

**http://192.168.145.128/**

Verified

- **jQuery UI 1.12.1**

- URL: <http://192.168.145.128/openemr/public/assets/jquery-ui/jquery-ui.js>
- Detection method: The library's name and version were determined based on the file's syntax fingerprint, and contents. Acunetix verified the library version and the associated vulnerabilities with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- CVE-ID: CVE-2021-41184
- Description: XSS in the 'of' option of the '.position()' util
- References:
  - <https://blog.jqueryui.com/2021/10/jquery-ui-1-13-0-released/>
  - <https://github.com/jquery/jquery-ui/security/advisories/GHSA-gpqq-952q-5327>

## Request

---

```
GET /openemr/public/assets/jquery-ui/jquery-ui.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/Documentation/help_files/openemr_installation_help.php
Cookie: OpenEMR=d40D5DeY1SqGsuSImcMvd1XbnUvSB1Sl%2CNIItqLcdHnpIKp4G
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

- **jQuery UI Datepicker 1.12.1**

- URL: <http://192.168.145.128/openemr/public/assets/jquery-ui/jquery-ui.js>
- Detection method: The library's name and version were determined based on the file's contents.
- CVE-ID: CVE-2021-41182, CVE-2021-41183
- Description: XSS in the 'altField' option of the Datepicker widget / XSS in '\*Text' options of the Datepicker widget
- References:
  - <https://blog.jqueryui.com/2021/10/jquery-ui-1-13-0-released/>
  - <https://github.com/jquery/jquery-ui/security/advisories/GHSA-9gj3-hwp5-pmw>
  - <https://github.com/jquery/jquery-ui/security/advisories/GHSA-j7qv-pgf6-hvh4>

## Request

---

```
GET /openemr/public/assets/jquery-ui/jquery-ui.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/Documentation/help_files/openemr_installation_help.php
Cookie: OpenEMR=d40D5DeY1SqGsuSImcMvd1XbnUvSB1S1%2CNItqLcdHnpIKp4G
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

- **jQuery 1.12.4**

- URL: <http://192.168.145.128/openemr/public/assets/jquery-ui/external/jquery/jquery.js>
- Detection method: The library's name and version were determined based on the file's syntax fingerprint, and contents. Acunetix verified the library version and the associated vulnerabilities with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- CVE-ID: CVE-2015-9251, CVE-2020-11022, CVE-2020-11023
- Description: Possible Cross Site Scripting via third-party text/javascript responses (1.12.0-1.12.2 mitigation reverted) / In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. / In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing option elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

- o References:

- <https://github.com/jquery/jquery/issues/2432>
- <https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/>
- <https://mksben.lo.cm/2020/05/jquery3.5.0-xss.html>
- <https://jquery.com/upgrade-guide/3.5/>
- <https://api.jquery.com/jQuery.htmlPrefilter/>
- <https://www.cvedetails.com/cve/CVE-2020-11022/>
- <https://github.com/advisories/GHSA-gxr4-xjj5-5px2>
- <https://www.cvedetails.com/cve/CVE-2020-11023/>
- <https://github.com/advisories/GHSA-jpcq-cgw6-v4j6>

## Request

---

```
GET /openemr/public/assets/jquery-ui/external/jquery/jquery.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/public/assets/jquery-ui/
Cookie: OpenEMR=6WeVd6ZCNQZ1gcdzS-0v%2CJShmKVZumFVDGJv2At8hAWUVeJ3
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

## <http://192.168.145.128/>

Verified

- **jQuery 1.10.2**

- o URL: <http://192.168.145.128/openemr/public/assets/jquery-datetimepicker/jquery.js>
- o Detection method: The library's name and version were determined based on the file's syntax fingerprint, and contents. Acunetix verified the library version and the associated vulnerabilities with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- o CVE-ID: CVE-2015-9251, CVE-2020-11022, CVE-2020-11023
- o Description: Possible Cross Site Scripting via third-party text/javascript responses / In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. / In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing option elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.
- o References:
  - <https://github.com/jquery/jquery/issues/2432>
  - <http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/>
  - <https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/>

- <https://mksben.l0.cm/2020/05/jquery3.5.0-xss.html>
- <https://jquery.com/upgrade-guide/3.5/>
- <https://api.jquery.com/jQuery.htmlPrefilter/>
- <https://www.cvedetails.com/cve/CVE-2020-11022/>
- <https://github.com/advisories/GHSA-gxr4-xjj5-5px2>
- <https://www.cvedetails.com/cve/CVE-2020-11023/>
- <https://github.com/advisories/GHSA-jpcq-cgw6-v4j6>

## Request

---

```
GET /openemr/public/assets/jquery-datetimepicker/jquery.js HTTP/1.1
Host: 192.168.145.128
accept: /*
accept-language: en-US
cookie: OpenEMR=SMoagLf26TS1Vx2PDvSGHTEJwG3t9eYeCWJyUPD7WNEu5a8X
Referer: http://192.168.145.128/openemr/public/assets/jquery-datetimepicker/
Accept-Encoding: gzip,deflate,br
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
```

<http://192.168.145.128/>

Verified

- **jQuery UI 1.8.10**

- URL: <http://192.168.145.128/openemr/interface/super/rules/www/js/cdr-multiselect/jquery-ui.min.js>
- Detection method: The library's name and version were determined based on the file's syntax fingerprint, and contents. Acunetix verified the library version and the associated vulnerabilities with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- CVE-ID: CVE-2021-41184
- Description: XSS in the 'of' option of the '.position()' util
- References:
  - <https://blog.jqueryui.com/2021/10/jquery-ui-1-13-0-released/>
  - <https://github.com/jquery/jquery-ui/security/advisories/GHSA-gpqq-952q-5327>

## Request

---

```
GET /openemr/interface/super/rules/www/js/cdr-multiselect/jquery-ui.min.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/interface/login_screen.php
Cookie: OpenEMR=2biStMm-fnsHdYMyYHQGKwzilsysHJvKUerLZszaOGdltFQQ
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
```

Host: 192.168.145.128  
Connection: Keep-alive

## <http://192.168.145.128/>

Verified

- **jQuery UI Dialog 1.8.10**

- URL: <http://192.168.145.128/openemr/interface/super/rules/www/js/cdr-multiselect/jquery-ui.min.js>
- Detection method: The library's name and version were determined based on the file's contents. Acunetix verified the library version and the associated vulnerabilities with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- CVE-ID: CVE-2010-5312, CVE-2016-7103
- Description: Title cross-site scripting vulnerability / XSS in dialog closeText
- References:
  - <http://bugs.jqueryui.com/ticket/6016>
  - <https://nodesecurity.io/advisories/127>
  - <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7103>
  - <https://www.cvedetails.com/cve/CVE-2016-7103/>

## Request

```
GET /openemr/interface/super/rules/www/js/cdr-multiselect/jquery-ui.min.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/interface/login_screen.php
Cookie: OpenEMR=2biStMm-fnsHdYMyYHQGKWzilsysHJvKUerLZszaOGdltFQQ
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

## <http://192.168.145.128/>

Verified

- **jQuery 1.5.1**

- URL: <http://192.168.145.128/openemr/interface/super/rules/www/js/cdr-multiselect/jquery.min.js>
- Detection method: The library's name and version were determined based on the file's syntax fingerprint, and contents. Acunetix verified the library version and the associated vulnerabilities with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- CVE-ID: CVE-2011-4969, CVE-2015-9251, CVE-2020-11022, CVE-2020-11023
- Description: Cross-site scripting (XSS) vulnerability in jQuery before 1.6.3, when using location.hash to select elements, allows remote attackers to inject arbitrary web script or HTML via a crafted tag. / Selector

interpreted as HTML / Possible Cross Site Scripting via third-party text/javascript responses / In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. / In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing option elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

- o References:

- <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4969>
- <http://research.insecurelabs.org/jquery/test/>
- <http://bugs.jquery.com/ticket/11290>
- <https://github.com/jquery/jquery/issues/2432>
- <http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/>
- <https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/>
- <https://mksben.l0.cm/2020/05/jquery3.5.0-xss.html>
- <https://jquery.com/upgrade-guide/3.5/>
- <https://api.jquery.com/jQuery.htmlPrefilter/>
- <https://www.cvedetails.com/cve/CVE-2020-11022/>
- <https://github.com/advisories/GHSA-gxr4-xjj5-5px2>
- <https://www.cvedetails.com/cve/CVE-2020-11023/>
- <https://github.com/advisories/GHSA-jpcq-cgw6-v4j6>

## Request

---

```
GET /openemr/interface/super/rules/www/js/cdr-multiselect/jquery.min.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/interface/login_screen.php
Cookie: OpenEMR=2biStMm-fnsHdYMyYHQGKwzilsysHJvKUerLZszaOGdltFQQ
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

<http://192.168.145.128/>

Verified

- **jQuery 1.4.3**

- o URL: [http://192.168.145.128/openemr/interface/modules/zend\\_modules/public/js/lib/jquery.treeview-1.4.1/lib/jquery.js](http://192.168.145.128/openemr/interface/modules/zend_modules/public/js/lib/jquery.treeview-1.4.1/lib/jquery.js)
- o Detection method: The library's name and version were determined based on the file's syntax fingerprint, and contents. Acunetix verified the library version and the associated vulnerabilities with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.

- CVE-ID: CVE-2011-4969, CVE-2015-9251, CVE-2020-11022, CVE-2020-11023
- Description: Cross-site scripting (XSS) vulnerability in jQuery before 1.6.3, when using location.hash to select elements, allows remote attackers to inject arbitrary web script or HTML via a crafted tag. / Selector interpreted as HTML / Possible Cross Site Scripting via third-party text/javascript responses / In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. / In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing option elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.
- References:
  - <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4969>
  - <http://research.insecurelabs.org/jquery/test/>
  - <http://bugs.jquery.com/ticket/11290>
  - <https://github.com/jquery/jquery/issues/2432>
  - <http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/>
  - <https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/>
  - <https://mksben.l0.cm/2020/05/jquery3.5.0-xss.html>
  - <https://jquery.com/upgrade-guide/3.5/>
  - <https://api.jquery.com/jQuery.htmlPrefilter/>
  - <https://www.cvedetails.com/cve/CVE-2020-11022/>
  - <https://github.com/advisories/GHSA-gxr4-xjj5-5px2>
  - <https://www.cvedetails.com/cve/CVE-2020-11023/>
  - <https://github.com/advisories/GHSA-jpcq-cgw6-v4j6>

## Request

---

```

GET /openemr/interface/modules/zend_modules/public/js/lib/jquery.treeview-1.4.1/lib/jquery.js
HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/interface/login_screen.php
Cookie: OpenEMR=2biStMm-fnsHdYMyYHQGKWzilsysHJvKUerLZszaOGdltFQQ
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
  
```

<http://192.168.145.128/>

Verified

- jQuery UI 1.11.4
  - URL: [http://192.168.145.128/openemr/interface/forms/eye\\_mag/js/jquery-ui-1-11-4/jquery-ui.min.js](http://192.168.145.128/openemr/interface/forms/eye_mag/js/jquery-ui-1-11-4/jquery-ui.min.js)

- Detection method: The library's name and version were determined based on the file's syntax fingerprint, and contents. Acunetix verified the library version and the associated vulnerabilities with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- CVE-ID: CVE-2021-41184
- Description: XSS in the 'of' option of the '.position()' util
- References:
  - <https://blog.jqueryui.com/2021/10/jquery-ui-1-13-0-released/>
  - <https://github.com/jquery/jquery-ui/security/advisories/GHSA-gpqq-952q-5327>

## Request

---

```
GET /openemr/interface/forms/eye_mag/js/jquery-ui-1-11-4/jquery-ui.min.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/interface/login_screen.php
Cookie: OpenEMR=2biStMm-fnsHdYMyYHQGKWzilsysHJvKUerLZszaOGdltFQQ
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

<http://192.168.145.128/>

Verified

### • jQuery UI Dialog 1.11.4

- URL: [http://192.168.145.128/openemr/interface/forms/eye\\_mag/js/jquery-ui-1-11-4/jquery-ui.min.js](http://192.168.145.128/openemr/interface/forms/eye_mag/js/jquery-ui-1-11-4/jquery-ui.min.js)
- Detection method: The library's name and version were determined based on the file's contents. Acunetix verified the library version and the associated vulnerabilities with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- CVE-ID: CVE-2016-7103
- Description: XSS in dialog closeText
- References:
  - <https://nodesecurity.io/advisories/127>
  - <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7103>
  - <https://www.cvedetails.com/cve/CVE-2016-7103/>

## Request

---

```
GET /openemr/interface/forms/eye_mag/js/jquery-ui-1-11-4/jquery-ui.min.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/interface/login_screen.php
```

Cookie: OpenEMR=2biStMm-fnsHdYMyYHQGKWzilsysHJvKUerLZszaOGdltFQQ  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
Accept-Encoding: gzip,deflate,br  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)  
Chrome/109.0.0.0 Safari/537.36  
Host: 192.168.145.128  
Connection: Keep-alive

## <http://192.168.145.128/> Verified

- **jQuery 1.8.0**

- URL: [http://192.168.145.128/openemr/interface/modules/zend\\_modules/public/js/lib/jquery-1.8.0.min.js](http://192.168.145.128/openemr/interface/modules/zend_modules/public/js/lib/jquery-1.8.0.min.js)
- Detection method: The library's name and version were determined based on the file's name, and contents. Acunetix verified the library version and the associated vulnerabilities with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- CVE-ID: CVE-2015-9251, CVE-2020-11022, CVE-2020-11023
- Description: Selector interpreted as HTML / Possible Cross Site Scripting via third-party text/javascript responses / In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. / In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing option elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.
- References:
  - <http://bugs.jquery.com/ticket/11290>
  - <http://research.insecurelabs.org/jquery/test/>
  - <https://github.com/jquery/jquery/issues/2432>
  - <http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/>
  - <https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/>
  - <https://mksben.l0.cm/2020/05/jquery3.5.0-xss.html>
  - <https://jquery.com/upgrade-guide/3.5/>
  - <https://api.jquery.com/jQuery.htmlPrefilter/>
  - <https://www.cvedetails.com/cve/CVE-2020-11022/>
  - <https://github.com/advisories/GHSA-gxr4-xjj5-5px2>
  - <https://www.cvedetails.com/cve/CVE-2020-11023/>
  - <https://github.com/advisories/GHSA-jpcq-cgw6-v4j6>

## Request

```
GET /openemr/interface/modules/zend_modules/public/js/lib/jquery-1.8.0.min.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/interface/login_screen.php
Cookie: OpenEMR=2biStMm-fnsHdYMyYHQGKWzilsysHJvKUerLZszaOGdltFQQ
```

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
Accept-Encoding: gzip,deflate,br  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)  
Chrome/109.0.0.0 Safari/537.36  
Host: 192.168.145.128  
Connection: Keep-alive

## <http://192.168.145.128/>

Verified

- **jQuery 1.8.2**

- URL: [http://192.168.145.128/openemr/interface/modules/zend\\_modules/public/js/lib/jquery-1.8.2.min.js](http://192.168.145.128/openemr/interface/modules/zend_modules/public/js/lib/jquery-1.8.2.min.js)
- Detection method: The library's name and version were determined based on the file's name, and contents. Acunetix verified the library version and the associated vulnerabilities with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- CVE-ID: CVE-2015-9251, CVE-2020-11022, CVE-2020-11023
- Description: Selector interpreted as HTML / Possible Cross Site Scripting via third-party text/javascript responses / In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. / In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing option elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.
- References:
  - <http://bugs.jquery.com/ticket/11290>
  - <http://research.insecurelabs.org/jquery/test/>
  - <https://github.com/jquery/jquery/issues/2432>
  - <http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/>
  - <https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/>
  - <https://mksben.lo.cm/2020/05/jquery3.5.0-xss.html>
  - <https://jquery.com/upgrade-guide/3.5/>
  - <https://api.jquery.com/jQuery.htmlPrefilter/>
  - <https://www.cvedetails.com/cve/CVE-2020-11022/>
  - <https://github.com/advisories/GHSA-gxr4-xjj5-5px2>
  - <https://www.cvedetails.com/cve/CVE-2020-11023/>
  - <https://github.com/advisories/GHSA-jpcq-cgw6-v4j6>

## Request

---

GET /openemr/interface/modules/zend\_modules/public/js/lib/jquery-1.8.2.min.js HTTP/1.1  
Acunetix-Aspect: enabled  
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7  
Acunetix-Aspect-ScanID: 1655702786608078775  
Acunetix-Aspect-Queries: aspectalerts;routes  
Referer: http://192.168.145.128/openemr/interface/login\_screen.php  
Cookie: OpenEMR=2biStMm-fnsHdYMyYHQGKwzilsysHJvKUerLZszaOGdltFQQ  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Encoding: gzip, deflate, br  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)  
Chrome/109.0.0.0 Safari/537.36  
Host: 192.168.145.128  
Connection: Keep-alive

## <http://192.168.145.128/> Verified

- **jQuery 1.8.3**

- URL: [http://192.168.145.128/openemr/interface/modules/zend\\_modules/public/js/lib/jquery-1.8.3.js](http://192.168.145.128/openemr/interface/modules/zend_modules/public/js/lib/jquery-1.8.3.js)
- Detection method: The library's name and version were determined based on the file's name, and contents. Acunetix verified the library version and the associated vulnerabilities with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- CVE-ID: CVE-2015-9251, CVE-2020-11022, CVE-2020-11023
- Description: Selector interpreted as HTML / Possible Cross Site Scripting via third-party text/javascript responses / In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. / In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing option elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.
- References:
  - <http://bugs.jquery.com/ticket/11290>
  - <http://research.insecurelabs.org/jquery/test/>
  - <https://github.com/jquery/jquery/issues/2432>
  - <http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/>
  - <https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/>
  - <https://mksben.l0.cm/2020/05/jquery3.5.0-xss.html>
  - <https://jquery.com/upgrade-guide/3.5/>
  - <https://api.jquery.com/jQuery.htmlPrefilter/>
  - <https://www.cvedetails.com/cve/CVE-2020-11022/>
  - <https://github.com/advisories/GHSA-gxr4-xjj5-5px2>
  - <https://www.cvedetails.com/cve/CVE-2020-11023/>
  - <https://github.com/advisories/GHSA-jpcq-cgw6-v4j6>

## Request

---

```
GET /openemr/interface/modules/zend_modules/public/js/lib/jquery-1.8.3.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58adee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/interface/login_screen.php
Cookie: OpenEMR=2biStMm-fnsHdYMyYHQGKWzilsysHJvKUerLZszaOGdltFQQ
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
```

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)  
Chrome/109.0.0.0 Safari/537.36  
Host: 192.168.145.128  
Connection: Keep-alive

## <http://192.168.145.128/>

Confidence: 80%

- **jQuery UI 1.9.2**
  - URL: [http://192.168.145.128/openemr/interface/modules/zend\\_modules/public/js/lib/jquery-ui.custom.js](http://192.168.145.128/openemr/interface/modules/zend_modules/public/js/lib/jquery-ui.custom.js)
  - Detection method: The library's name and version were determined based on the file's contents. Acunetix performed a syntax analysis of the file and detected functional differences between the file and the original library version. As the file was likely modified on purpose, the confidence level of the vulnerability alert has been lowered.
  - CVE-ID: CVE-2021-41184
  - Description: XSS in the 'of' option of the '.position()' util
  - References:
    - <https://blog.jqueryui.com/2021/10/jquery-ui-1-13-0-released/>
    - <https://github.com/jquery/jquery-ui/security/advisories/GHSA-gpqq-952q-5327>

## Request

GET /openemr/interface/modules/zend\_modules/public/js/lib/jquery-ui.custom.js HTTP/1.1  
Acunetix-Aspect: enabled  
Acunetix-Aspect-Password: d4d608fef00a58adee3950d33ced68a7  
Acunetix-Aspect-ScanID: 1655702786608078775  
Acunetix-Aspect-Queries: aspectalerts;routes  
Referer: http://192.168.145.128/openemr/interface/login\_screen.php  
Cookie: OpenEMR=2biStMm-fnsHdYMyYHQGKwzilysHJvKUerLZszaOGdltFQQ  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
Accept-Encoding: gzip,deflate,br  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)  
Chrome/109.0.0.0 Safari/537.36  
Host: 192.168.145.128  
Connection: Keep-alive

## <http://192.168.145.128/>

Confidence: 95%

- **jQuery UI Datepicker 1.9.2**
  - URL: [http://192.168.145.128/openemr/interface/modules/zend\\_modules/public/js/lib/jquery-ui.custom.js](http://192.168.145.128/openemr/interface/modules/zend_modules/public/js/lib/jquery-ui.custom.js)
  - Detection method: The library's name and version were determined based on the file's contents.
  - CVE-ID: CVE-2021-41182, CVE-2021-41183
  - Description: XSS in the 'altField' option of the Datepicker widget / XSS in '\*Text' options of the Datepicker widget
  - References:

- <https://blog.jqueryui.com/2021/10/jquery-ui-1-13-0-released/>
- <https://github.com/jquery/jquery-ui/security/advisories/GHSA-9gj3-hwp5-pmw>
- <https://github.com/jquery/jquery-ui/security/advisories/GHSA-j7qv-pgf6-hvh4>

## Request

---

```
GET /openemr/interface/modules/zend_modules/public/js/lib/jquery-ui.custom.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/interface/login_screen.php
Cookie: OpenEMR=2biStMm-fnsHdYMyYHQGKWzilsysHJvKUerLZszaOGdltFQQ
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

**http://192.168.145.128/**

Verified

- **jQuery UI 1.10.3**

- URL: [http://192.168.145.128/openemr/interface/modules/zend\\_modules/public/js/lib/jquery-ui.js](http://192.168.145.128/openemr/interface/modules/zend_modules/public/js/lib/jquery-ui.js)
- Detection method: The library's name and version were determined based on the file's syntax fingerprint, and contents. Acunetix verified the library version and the associated vulnerabilities with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- CVE-ID: CVE-2021-41184
- Description: XSS in the 'of' option of the '.position()' util
- References:
  - <https://blog.jqueryui.com/2021/10/jquery-ui-1-13-0-released/>
  - <https://github.com/jquery/jquery-ui/security/advisories/GHSA-gpqq-952q-5327>

## Request

---

```
GET /openemr/interface/modules/zend_modules/public/js/lib/jquery-ui.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/interface/login_screen.php
Cookie: OpenEMR=2biStMm-fnsHdYMyYHQGKWzilsysHJvKUerLZszaOGdltFQQ
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
```

<http://192.168.145.128/>

Verified

- jQuery UI Dialog 1.10.3

- URL: http://192.168.145.128/openemr/interface/modules/zend\_modules/public/js/lib/jquery-ui.js
- Detection method: The library's name and version were determined based on the file's contents. Acunetix verified the library version and the associated vulnerabilities with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- CVE-ID: CVE-2016-7103
- Description: XSS in dialog closeText
- References:
  - <https://nodesecurity.io/advisories/127>
  - <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7103>
  - <https://www.cvedetails.com/cve/CVE-2016-7103/>

## Request

---

```

GET /openemr/interface/modules/zend_modules/public/js/lib/jquery-ui.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/interface/login_screen.php
Cookie: OpenEMR=2biStMm-fnsHdYMyYHQGKWzilsysHJvKUerLZszaOGdltFQQ
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
  
```

<http://192.168.145.128/>

Confidence: 95%

- jQuery UI Datepicker 1.10.3

- URL: http://192.168.145.128/openemr/interface/modules/zend\_modules/public/js/lib/jquery-ui.js
- Detection method: The library's name and version were determined based on the file's contents.
- CVE-ID: CVE-2021-41182, CVE-2021-41183
- Description: XSS in the 'altField' option of the Datepicker widget / XSS in '\*Text' options of the Datepicker widget
- References:
  - <https://blog.jqueryui.com/2021/10/jquery-ui-1-13-0-released/>
  - <https://github.com/jquery/jquery-ui/security/advisories/GHSA-9gj3-hwp5-pmwc>
  - <https://github.com/jquery/jquery-ui/security/advisories/GHSA-j7qv-pgf6-hvh4>

## Request

---

```
GET /openemr/interface/modules/zend_modules/public/js/lib/jquery-ui.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/interface/login_screen.php
Cookie: OpenEMR=2biStMm-fnsHdYMyYHQGKwzilsysHJvKUerLZszaOGdltFQQ
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

## Recommendation

---

Upgrade to the latest version.

## Outdated JavaScript libraries

---

You are using an outdated version of one or more JavaScript libraries. A more recent version is available. Although your version was not found to be affected by any security vulnerabilities, it is recommended to keep libraries up to date.

### CWE

CWE-937

### CVSS2

AV:N/AC:H/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	High
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

### CVSS3

CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	High
Privileges Required	None
User Interaction	Required
Scope	Changed
Confidentiality	None
Integrity Impact	None
Availability Impact	None

## Impact

---

## <http://10.10.236.31/>

Verified

- **jQuery UI Dialog 1.12.1**

- URL: <http://10.10.236.31/openemr/public/assets/jquery-ui/jquery-ui.js>
- Detection method: The library's name and version were determined based on the file's contents. Acunetix verified the library version with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- References:
  - <https://jqueryui.com/download/>

### Request

```
GET /openemr/public/assets/jquery-ui/jquery-ui.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 8595e182db21cbbc10c83c2c4cf193d3
Acunetix-Aspect-ScanID: 816589585389164376
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://10.10.236.31/openemr/Documentation/help_files/openemr_installation_help.php
Cookie: OpenEMR=b3DHM9s5BR72IjC3y6GcpBb736abtMj3%2CfzaSNeoS-j94pMx
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 10.10.236.31
Connection: Keep-alive
```

## <http://10.10.236.31/>

Verified

- **jQuery UI Tooltip 1.12.1**

- URL: <http://10.10.236.31/openemr/public/assets/jquery-ui/jquery-ui.js>
- Detection method: The library's name and version were determined based on the file's contents. Acunetix verified the library version with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- References:
  - <https://jqueryui.com/download/>

### Request

```
GET /openemr/public/assets/jquery-ui/jquery-ui.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 8595e182db21cbbc10c83c2c4cf193d3
Acunetix-Aspect-ScanID: 816589585389164376
Acunetix-Aspect-Queries: aspectalerts;routes
```

Referer: http://10.10.236.31/openemr/Documentation/help\_files/openemr\_installation\_help.php  
Cookie: OpenEMR=b3DHM9s5BR72IjC3y6GcpBb736abtMj3%2CfzaSNeoS-j94pMx  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
Accept-Encoding: gzip,deflate,br  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)  
Chrome/109.0.0.0 Safari/537.36  
Host: 10.10.236.31  
Connection: Keep-alive

## <http://192.168.145.128/>

Verified

- **jQuery UI Dialog 1.12.1**

- URL: <http://192.168.145.128/openemr/public/assets/jquery-ui/jquery-ui.js>
- Detection method: The library's name and version were determined based on the file's contents. Acunetix verified the library version with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- References:
  - <https://jqueryui.com/download/>

## Request

---

GET /openemr/public/assets/jquery-ui/jquery-ui.js HTTP/1.1  
Acunetix-Aspect: enabled  
Acunetix-Aspect-Password: d4d608fef00a58adee3950d33ced68a7  
Acunetix-Aspect-ScanID: 1655702786608078775  
Acunetix-Aspect-Queries: aspectalerts;routes  
Referer: http://192.168.145.128/openemr/Documentation/help\_files/openemr\_installation\_help.php  
Cookie: OpenEMR=d40D5DeY1SqGsuSImcMvd1XbnUvSB1S1%2CNItqLcdHnpIKp4G  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
Accept-Encoding: gzip,deflate,br  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)  
Chrome/109.0.0.0 Safari/537.36  
Host: 192.168.145.128  
Connection: Keep-alive

## <http://192.168.145.128/>

Verified

- **jQuery UI Tooltip 1.12.1**

- URL: <http://192.168.145.128/openemr/public/assets/jquery-ui/jquery-ui.js>
- Detection method: The library's name and version were determined based on the file's contents. Acunetix verified the library version with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- References:
  - <https://jqueryui.com/download/>

## Request

---

```
GET /openemr/public/assets/jquery-ui/jquery-ui.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58ad3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/Documentation/help_files/openemr_installation_help.php
Cookie: OpenEMR=d40D5DeY1SqGsuSImcMvd1XbnUvSB1S1%2CNItgLcdHnpIKp4G
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

**http://192.168.145.128/**

Verified

- **jQuery UI Tooltip 1.11.4**

- URL: [http://192.168.145.128/openemr/interface/forms/eye\\_mag/js/jquery-ui-1-11-4/jquery-ui.min.js](http://192.168.145.128/openemr/interface/forms/eye_mag/js/jquery-ui-1-11-4/jquery-ui.min.js)
- Detection method: The library's name and version were determined based on the file's contents. Acunetix verified the library version with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- References:
  - <https://jqueryui.com/download/>

## Request

---

```
GET /openemr/interface/forms/eye_mag/js/jquery-ui-1-11-4/jquery-ui.min.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58ad3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/interface/login_screen.php
Cookie: OpenEMR=2biStMm-fnsHdYMyYHQGKwzilsysHJvKUerLZszaOGdltFQQ
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

**http://192.168.145.128/**

Verified

- **jQuery UI Tooltip 1.10.3**

- URL: [http://192.168.145.128/openemr/interface/modules/zend\\_modules/public/js/lib/jquery-ui.js](http://192.168.145.128/openemr/interface/modules/zend_modules/public/js/lib/jquery-ui.js)
- Detection method: The library's name and version were determined based on the file's contents. Acunetix verified the library version with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- References:
  - <https://jqueryui.com/download/>

## Request

---

```
GET /openemr/interface/modules/zend_modules/public/js/lib/jquery-ui.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/interface/login_screen.php
Cookie: OpenEMR=2biStMm-fnsHdYMyYHQGKwzilsysHJvKUerLZszaOGdltFQQ
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

## <http://192.168.145.128/>

Confidence: 95%

- **Modernizr 2.6.2**

- URL: [http://192.168.145.128/openemr/interface/modules/zend\\_modules/public/js/lib/modernizr-2.6.2.min.js](http://192.168.145.128/openemr/interface/modules/zend_modules/public/js/lib/modernizr-2.6.2.min.js)
- Detection method: The library's name and version were determined based on the file's name.
- References:
  - <https://github.com/Modernizr/Modernizr/releases>

## Request

---

```
GET /openemr/interface/modules/zend_modules/public/js/lib/modernizr-2.6.2.min.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/interface/login_screen.php
Cookie: OpenEMR=2biStMm-fnsHdYMyYHQGKwzilsysHJvKUerLZszaOGdltFQQ
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

## Recommendation

Upgrade to the latest version.

# SI-10 INFORMATION INPUT VALIDATION

The information system checks the validity of organization-defined information inputs

**No alerts in this category**

# SI-11 ERROR HANDLING

The information system generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries; and reveals error messages only to organization-defined personnel or roles

## Application error messages

This alert requires manual confirmation

Acunetix found one or more error/warning messages. Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

These messages may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page(s).

### CWE

CWE-209

### CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

### CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low

<b>Integrity Impact</b>	None
<b>Availability Impact</b>	None

## Impact

---

Error messages may disclose sensitive information which can be used to escalate attacks.

### <http://10.10.236.31/>

Application error messages:

- http://10.10.236.31/openemr/interface/main/main\_screen.php  
**Unknown column 'Array' in 'where clause'**
- http://10.10.236.31/openemr/interface/main/main\_screen.php  
**<b>Warning</b>: include\_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php): failed to open stream: No such file or directory in <b>/var/www/html/openemr/interface/main/main\_screen.php</b> on line <b>5137</b><br />**
- http://10.10.236.31/openemr/interface/main/main\_screen.php  
**<b>Warning</b>: include\_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion (include\_path='/var/www/html/openemr/vendor/pear/archive\_tar:/var/www/html/openemr/vendor/pear/console\_getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear\_exception:::/usr/share/php') in <b>/var/www/html/openemr/interface/main/main\_screen.php</b> on line <b>5137</b><br />**
- http://10.10.236.31/openemr/interface/main/main\_screen.php  
**Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion**
- http://10.10.236.31/openemr/interface/main/messages/messages.php  
**<b>Warning</b>: include\_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php): failed to open stream: No such file or directory in <b>/var/www/html/openemr/interface/main/messages/messages.php</b> on line <b>5137</b><br />**
- http://10.10.236.31/openemr/interface/main/messages/messages.php  
**<b>Warning</b>: include\_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion (include\_path='/var/www/html/openemr/vendor/pear/archive\_tar:/var/www/html/openemr/vendor/pear/console\_getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear\_exception:::/usr/share/php') in <b>/var/www/html/openemr/interface/main/messages/messages.php</b> on line <b>5137</b><br />**
- http://10.10.236.31/openemr/interface/main/messages/messages.php  
**Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion**

## inclusion

- http://10.10.236.31/openemr/library/ajax/dated\_reminders\_counter.php  
**<b>Warning</b>: include\_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php): failed to open stream: No such file or directory in**  
**<b>/var/www/html/openemr/library/ajax/dated\_reminders\_counter.php</b> on line <b>5137</b><br />**
- http://10.10.236.31/openemr/library/ajax/dated\_reminders\_counter.php  
**<b>Warning</b>: include\_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion**  
**(include\_path='/var/www/html/openemr/vendor/pear/archive\_tar:/var/www/html/openemr/vendor/pear/console getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear\_exception:::/usr/share/php') in**  
**<b>/var/www/html/openemr/library/ajax/dated\_reminders\_counter.php</b> on line <b>5137</b><br />**
- http://10.10.236.31/openemr/library/ajax/dated\_reminders\_counter.php  
**Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion**
- http://10.10.236.31/openemr/library/ajax/i18n\_generator.php  
**<b>Warning</b>: include\_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php): failed to open stream: No such file or directory in**  
**<b>/var/www/html/openemr/library/ajax/i18n\_generator.php</b> on line <b>5137</b><br />**
- http://10.10.236.31/openemr/library/ajax/i18n\_generator.php  
**<b>Warning</b>: include\_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion**  
**(include\_path='/var/www/html/openemr/vendor/pear/archive\_tar:/var/www/html/openemr/vendor/pear/console getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear\_exception:::/usr/share/php') in**  
**<b>/var/www/html/openemr/library/ajax/i18n\_generator.php</b> on line <b>5137</b><br />**
- http://10.10.236.31/openemr/library/ajax/i18n\_generator.php  
**Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion**
- http://10.10.236.31/openemr/interface/main/calendar/index.php  
**<b>Warning</b>: include\_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php): failed to open stream: No such file or directory in**  
**<b>/var/www/html/openemr/interface/main/calendar/index.php</b> on line <b>5137</b><br />**
- http://10.10.236.31/openemr/interface/main/calendar/index.php  
**<b>Warning</b>: include\_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion**  
**(include\_path='/var/www/html/openemr/vendor/pear/archive\_tar:/var/www/html/openemr/vendor/pear/console getopt:/var/www/html/openemr/vendor/pear/pear-core-**

- minimal/src:/var/www/html/openemr/vendor/pear/pear\_exception:::/usr/share/php') in  
**< b >/var/www/html/openemr/interface/main/calendar/index.php</b>** on line **< b >5137</b><br />**
- http://10.10.236.31/openemr/interface/main/calendar/index.php  
**< b >Warning</b>: include\_once('/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion**  
**< b >/var/www/html/openemr/interface/main/calendar/index.php</b>** on line **< b >5137</b><br />**
  - http://10.10.236.31/openemr/interface/login/login.php  
**< b >Warning</b>: include\_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion**  
**(include\_path='var/www/html/openemr/vendor/pear/archive\_tar:/var/www/html/openemr/vendor/pear/console\_getopt:/var/www/html/openemr/vendor/pear/pear-core-**  
minimal/src:/var/www/html/openemr/vendor/pear/pear\_exception:::/usr/share/php') in  
**< b >/var/www/html/openemr/interface/login/login.php</b>** on line **< b >5137</b><br />**
  - http://10.10.236.31/openemr/interface/login/login.php  
**Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion**
  - http://10.10.236.31/openemr/interface/main/tabs/main.php  
**< b >Warning</b>: include\_once('/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion**  
**< b >/var/www/html/openemr/interface/main/tabs/main.php</b>** on line **< b >5137</b><br />**
  - http://10.10.236.31/openemr/interface/main/tabs/main.php  
**< b >Warning</b>: include\_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion**  
**(include\_path='var/www/html/openemr/vendor/pear/archive\_tar:/var/www/html/openemr/vendor/pear/console\_getopt:/var/www/html/openemr/vendor/pear/pear-core-**  
minimal/src:/var/www/html/openemr/vendor/pear/pear\_exception:::/usr/share/php') in  
**< b >/var/www/html/openemr/interface/main/tabs/main.php</b>** on line **< b >5137</b><br />**

## Request

---

```
POST /openemr/interface/main/main_screen.php?auth=login&site=default HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://10.10.236.31/openemr
Cookie: OpenEMR=bbs8OgzIFbvo7hR%2Cj5ZvMq%2C3QTQmauASLmo3p3YX9WgoZJp2
```

Content-Length: 72  
Accept-Encoding: gzip, deflate, br  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)  
Chrome/109.0.0.0 Safari/537.36  
Host: 10.10.236.31  
Connection: Keep-alive

authUser[] = 1 & clearPass = 1 & languageChoice = 1 & new\_login\_session\_management = 1

## <http://192.168.145.128/>

Application error messages:

- http://192.168.145.128/openemr/interface/main/main\_screen.php  
**<b>Warning</b>: include\_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php): failed to open stream: No such file or directory in**  
**<b>/var/www/html/openemr/interface/main/main\_screen.php</b> on line <b>5137</b><br />**
- http://192.168.145.128/openemr/interface/main/main\_screen.php  
**<b>Warning</b>: include\_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion**  
**(include\_path='/var/www/html/openemr/vendor/pear/archive\_tar:/var/www/html/openemr/vendor/pear/console\_getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear\_exception:::/usr/share/php') in**  
**<b>/var/www/html/openemr/interface/main/main\_screen.php</b> on line <b>5137</b><br />**
- http://192.168.145.128/openemr/interface/main/main\_screen.php  
**Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion**
- http://192.168.145.128/openemr/interface/main/messages/messages.php  
**<b>Warning</b>: include\_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php): failed to open stream: No such file or directory in**  
**<b>/var/www/html/openemr/interface/main/messages/messages.php</b> on line <b>5137</b><br />**
- http://192.168.145.128/openemr/interface/main/messages/messages.php  
**<b>Warning</b>: include\_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion**  
**(include\_path='/var/www/html/openemr/vendor/pear/archive\_tar:/var/www/html/openemr/vendor/pear/console\_getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear\_exception:::/usr/share/php') in**  
**<b>/var/www/html/openemr/interface/main/messages/messages.php</b> on line <b>5137</b><br />**
- http://192.168.145.128/openemr/interface/main/messages/messages.php  
**Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion**

- http://192.168.145.128/openemr/library/ajax/dated\_reminders\_counter.php
 

**<b>Warning</b>: include\_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php): failed to open stream: No such file or directory in**

**<b>/var/www/html/openemr/library/ajax/dated\_reminders\_counter.php</b> on line <b>5137</b><br />**
- http://192.168.145.128/openemr/library/ajax/dated\_reminders\_counter.php
 

**<b>Warning</b>: include\_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion**

**(include\_path='/var/www/html/openemr/vendor/pear/archive\_tar:/var/www/html/openemr/vendor/pear/console\_getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear\_exception:::/usr/share/php') in**

**<b>/var/www/html/openemr/library/ajax/dated\_reminders\_counter.php</b> on line <b>5137</b><br />**
- http://192.168.145.128/openemr/library/ajax/dated\_reminders\_counter.php
 

**Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion**
- http://192.168.145.128/openemr/interface/login/login.php
 

**<b>Warning</b>: include\_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php): failed to open stream: No such file or directory in**

**<b>/var/www/html/openemr/interface/login/login.php</b> on line <b>5137</b><br />**
- http://192.168.145.128/openemr/interface/login/login.php
 

**<b>Warning</b>: include\_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion**

**(include\_path='/var/www/html/openemr/vendor/pear/archive\_tar:/var/www/html/openemr/vendor/pear/console\_getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear\_exception:::/usr/share/php') in**

**<b>/var/www/html/openemr/interface/login/login.php</b> on line <b>5137</b><br />**
- http://192.168.145.128/openemr/interface/login/login.php
 

**Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion**
- http://192.168.145.128/openemr/library/ajax/i18n\_generator.php
 

**<b>Warning</b>: include\_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php): failed to open stream: No such file or directory in**

**<b>/var/www/html/openemr/library/ajax/i18n\_generator.php</b> on line <b>5137</b><br />**
- http://192.168.145.128/openemr/library/ajax/i18n\_generator.php
 

**<b>Warning</b>: include\_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion**

**(include\_path='/var/www/html/openemr/vendor/pear/archive\_tar:/var/www/html/openemr/vendor/pear/console\_getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear\_exception:::/usr/share/php') in**

**<b>/var/www/html/openemr/library/ajax/i18n\_generator.php</b> on line <b>5137</b><br />**

- http://192.168.145.128/openemr/library/ajax/i18n\_generator.php  
**Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion**
- http://192.168.145.128/openemr/interface/login\_screen.php  
**<b>Warning</b>: include\_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php): failed to open stream: No such file or directory in <b>/var/www/html/openemr/interface/login\_screen.php</b> on line <b>5137</b><br />**
- http://192.168.145.128/openemr/interface/login\_screen.php  
**<b>Warning</b>: include\_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion  
(include\_path='/var/www/html/openemr/vendor/pear/archive\_tar:/var/www/html/openemr/vendor/pear/console\_getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear\_exception:::/usr/share/php') in <b>/var/www/html/openemr/interface/login\_screen.php</b> on line <b>5137</b><br />**
- http://192.168.145.128/openemr/interface/login\_screen.php  
**Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion**
- http://192.168.145.128/openemr/interface/main/dated\_reminders/dated\_reminders.php  
**<b>Warning</b>: include\_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php): failed to open stream: No such file or directory in <b>/var/www/html/openemr/interface/main/dated\_reminders/dated\_reminders.php</b> on line <b>5137</b><br />**
- http://192.168.145.128/openemr/interface/main/dated\_reminders/dated\_reminders.php  
**<b>Warning</b>: include\_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion  
(include\_path='/var/www/html/openemr/vendor/pear/archive\_tar:/var/www/html/openemr/vendor/pear/console\_getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear\_exception:::/usr/share/php') in <b>/var/www/html/openemr/interface/main/dated\_reminders/dated\_reminders.php</b> on line <b>5137</b><br />**
- http://192.168.145.128/openemr/interface/main/dated\_reminders/dated\_reminders.php  
**Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli\_log.inc.php' for inclusion**

## Request

---

```
GET /openemr/interface/main/main_screen.php HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
```

Acunetix-Aspect-ScanID: 1655702786608078775  
Acunetix-Aspect-Queries: filelist;packages;aspectalerts;routes  
Referer: http://192.168.145.128/openemr  
Cookie: OpenEMR=fLVw-dnCSU123MMDJ4XDEmokIFFZN%2CUpmA0oNxhYR1Fnqazp  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
Accept-Encoding: gzip,deflate,br  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)  
Chrome/109.0.0.0 Safari/537.36  
Host: 192.168.145.128  
Connection: Keep-alive

## Recommendation

---

Verify that these page(s) are disclosing error or warning messages and properly configure the application to log errors to a file instead of displaying the error to the user.

## Description

---

While information disclosure vulnerabilities are not directly exploitable by an attacker, they may help an attacker to learn about system specific information. The following is a list of **some** of the information an attacker may be able to obtain from application error disclosure.

- Internal IP addresses
- Secrets (passwords, keys, tokens...)
- Operating system distributions
- Software version numbers
- Missing security patches
- Application stack traces
- SQL statements
- Location of sensitive files (backups, temporary files...)
- Location of sensitive resources (databases, caches, code repositories...)

## References

---

### [PHP Runtime Configuration](#)

<https://www.php.net/manual/en/errorfunc.configuration.php#ini.display-errors>

### [Improper Error Handling](#)

[https://www.owasp.org/index.php/Improper\\_Error\\_Handling](https://www.owasp.org/index.php/Improper_Error_Handling)

## Error page web server version disclosure

---

Application errors or warning messages may disclose sensitive information about an application's internal workings to an attacker.

Acunetix found the web server version number and a list of modules enabled on the target server. Consult the 'Attack details' section for more information about the affected page.

## CWE

CWE-200

### CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

### CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

## Impact

Error messages information about an application's internal workings may be used to escalate attacks.

### <http://10.10.236.31/>

#### Request

```
GET /KnNz3PhQmq HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 10.10.236.31
Connection: Keep-alive
```

### <http://192.168.145.128/>

#### Request

```
GET /OSEbyESLkq HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

## Recommendation

---

Properly configure the web server not to disclose information about an application's internal workings to the user. Consult the 'Web references' section for more information.

## References

---

### [Custom Error Responses \(Apache HTTP Server\)](#)

<https://httpd.apache.org/docs/current/custom-error.html>

### [server\\_tokens \(Nginx\)](#)

[http://nginx.org/en/docs/http/ngx\\_http\\_core\\_module.html#server\\_tokens](http://nginx.org/en/docs/http/ngx_http_core_module.html#server_tokens)

### [Remove Unwanted HTTP Response Headers \(Microsoft IIS\)](#)

<https://blogs.msdn.microsoft.com/varunm/2013/04/23/remove-unwanted-http-response-headers/>

## SI-15 INFORMATION OUTPUT FILTERING

---

The information system validates information output from organization-defined software programs and/or applications to ensure that the information is consistent with the expected content.

**No alerts in this category**

## SI-16 MEMORY PROTECTION

---

The information system implements organization-defined security safeguards to protect its memory from unauthorized code execution

**No alerts in this category**

## Coverage

---

http://192.168.145.128/

http://192.168.145.128/openemr/

http://192.168.145.128/openemr/public/assets/checklist-model/

http://192.168.145.128/openemr/vendor/

http://10.10.236.31/

http://10.10.236.31/openemr/

http://10.10.236.31/openemr/vendor/