usd AG Security Advisories 11/2021

From: Responsible Disclosure via Fulldisclosure <fulldisclosure () seclists org>
Date: Fri, 3 Dec 2021 15:15:40 +0000

Hi all,

this week usd AG disclosed the following advisories at
<https://herolab.usd.de/security-advisories/>
https://herolab.usd.de/security-advisories/:

* usd-2021-0032 | XSS in SUSE CVE Database (suse.com):
<https://herolab.usd.de/security-advisories/usd-2021-0032/>
https://herolab.usd.de/security-advisories/usd-2021-0032/

* usd-2021-0006 | LFI & Path Traversal in ChronoEngine ChronoForms v7:
<https://herolab.usd.de/security-advisories/usd-2021-0006/>
https://herolab.usd.de/security-advisories/usd-2021-0006/

* usd-2021-0007 | LFI & Path Traversal in ChronoEngine ChronoForums:
<https://herolab.usd.de/security-advisories/usd-2021-0007/>
https://herolab.usd.de/security-advisories/usd-2021-0007/

* usd-2020-0106 (CVE-2021-25273) | XSS in Sophos UTM:
<https://herolab.usd.de/security-advisories/usd-2020-0106/>
https://herolab.usd.de/security-advisories/usd-2020-0106/

----

usd-2021-0032 | SUSE CVE Database (suse.com)

==

Advisory ID: usd-2021-0032

Affected Product: SUSE CVE database

Vulnerability Type: CWE-79: Improper Neutralization of Input During Web Page
Generation (‚Cross-site Scripting')

Security Risk: High

Vendor URL: <https://www.suse.com/security/cve/>
https://www.suse.com/security/cve/

Vendor Status: Fixed

Suse's CVE database embedded third-party contents without sufficient
filtering and/or encoding. Multiple incidents have been identified where
Suse embedded untrusted <script> tags, resulting in stored
Cross-Site-Scripting (XSS).

Proof of Concept (PoC)

======================

In order to exploit the vulnerability, a new CVE record must be published
officially. This CVE record can contain arbitrary text as a "description".
Here, JavaScript code can injected. The SUSE CVE database imports this data
automatically and displays the information on a website. The injected code
will be executed automatically.

An example CVE containing an HTML <script> tag is CVE-2021-32718 (
<https://www.suse.com/security/cve/CVE-2021-32718.html>
https://www.suse.com/security/cve/CVE-2021-32718.html). Here, the HTML tag
was interpreted and potentially malicious JavaScript code which could follow
here would have been executed.

The following screenshots illustrate that the <script> tag was embedded
without any encoding or filtering and interpreted as markup by the browser
accordingly:

 <https://herolab.usd.de/wp-content/uploads/sites/9/2021/11/suse_xss1.png>
https://herolab.usd.de/wp-content/uploads/sites/9/2021/11/suse_xss1.png

 <https://herolab.usd.de/wp-content/uploads/sites/9/2021/11/suse_xss4.png>
https://herolab.usd.de/wp-content/uploads/sites/9/2021/11/suse_xss4.png

Credits

=======

This security vulnerability was found by Christian Rellmann of usd AG.

Please find the full advisory here:
<https://herolab.usd.de/security-advisories/usd-2021-0032/>
https://herolab.usd.de/security-advisories/usd-2021-0032/

----

usd-2021-0006 | ChronoEngine ChronoForms v7
===

Advisory ID: usd20210006

Affected Product: ChronoEngine ChronoForms v7

Affected Version: v7.0.7

Vulnerability Type: CWE-22: Improper Limitation of a Pathname to a Restricted Directory (‚Path Traversal')

Security Risk: Medium

Vendor URL: <https://www.chronoengine.com/chronoforms>
https://www.chronoengine.com/chronoforms

Vendor Status: Unknown

The ChronoForms function to download form input logs is vulnerable through path traversal attacks. This allows an attacker with administration permissions to download arbitrary files from web servers filesystem.

The parameter `fname` passed to the log script in the Joomla administration interface is not filtered for path traversal. This allows an attacker with administration permissions to download arbitrary files from the web servers filesystem, like for instance Joomla's configuration file containing secret credentials.

Proof of Concept (PoC)
======================

Open the vulnerable file in a Webbrowser:
<https://%3cJoomlaInstallation%3e/administrator/index.php?option=com_chronoforms7&cont=logs&act=file&fname=%3clocal_file>
https://<JoomlaInstallation>/administrator/index.php?option=com_chronoforms7&cont=logs&act=file&fname=<local_file>

Examples:

* /etc/passwd:
<https://herolab.usd.de/wp-content/uploads/sites/9/2021/11/usd20210006-1-redacted.png>
https://herolab.usd.de/wp-content/uploads/sites/9/2021/11/usd20210006-1-redacted.png

* Joomla Configuration:
<https://herolab.usd.de/wp-content/uploads/sites/9/2021/11/usd20210006-2-redacted.png>
https://herolab.usd.de/wp-content/uploads/sites/9/2021/11/usd20210006-2-redacted.png

Credits
=======

This security vulnerability was found by Nicolas Schickert and Tim Kranz of usd AG.

Please find the full advisory here:
<https://herolab.usd.de/security-advisories/usd-2021-0006/>
https://herolab.usd.de/security-advisories/usd-2021-0006/

----

usd-2021-0007 | ChronoEngine ChronoForums
===

Advisory ID: usd20210007

Affected Product: ChronoEngine ChronoForums

Affected Version: v2.0.11

Vulnerability Type: CWE-22: Improper Limitation of a Pathname to a Restricted Directory (‚Path Traversal')

Security Risk: High

Vendor URL: <https://www.chronoengine.com/chronoforums>
https://www.chronoengine.com/chronoforums

Vendor Status: Unknown

The ChronoForums avatar function is vulnerable through unauthenticated path traversal attacks. This enables unauthenticated attackers to read arbitrary files, like for instance Joomla's configuration file containing secret credentials.

The ChronoForums avatar function is vulnerable through path traversal attacks. An attacker can pass arbitrary local file paths as 'av' parameter. The content of the file is returned. Unauthenticated attackers could use this vulnerability to read arbitrary files, like for instance Joomla's configuration file containing secret credentials.

Proof of Concept (PoC)
======================

Open the vulnerable file in a webbrowser:
<https://%3cJoomlaInstallation%3e/index.php/component/chronoforums2/profiles/avatar/u1?tvout=file&av=%3clocal_file>
https://<JoomlaInstallation>/index.php/component/chronoforums2/profiles/avatar/u1?tvout=file&av=<local_file>

Examples:

* `../../../../../../../etc/passwd`:
<https://herolab.usd.de/wp-content/uploads/sites/9/2021/11/usd20210007-1.png
https://herolab.usd.de/wp-content/uploads/sites/9/2021/11/usd20210007-1.png

* `../../../../configuration.php`:
<https://herolab.usd.de/wp-content/uploads/sites/9/2021/11/usd20210007-2.png
https://herolab.usd.de/wp-content/uploads/sites/9/2021/11/usd20210007-2.png

Credits

=======

This security vulnerability was found by Nicolas Schickert and Tim Kranz of usd AG.

Please find the full advisory here:
<https://herolab.usd.de/security-advisories/usd-2021-0006/>
https://herolab.usd.de/security-advisories/usd-2021-0006/

----

usd-2020-0106 (CVE-2021-25273) | Sophos UTM

===

Advisory ID: usd-2020-0106

CWE ID: CVE-2021-25273

Affected Product: Sophos UTM

Affected Version: < UTM 9.706

Vulnerability Type: CWE-79: Improper Neutralization of Input During Web Page Generation (‚Cross-site Scripting')

Security Risk: Medium

Vendor URL: <https://sophos.com> https://sophos.com

Vendor Status: Fixed

Sophos UTM offers a web interface to manage quarantined mails. The web-based interface did not filter user controlled inputs sufficiently, resulting in multiple Cross-Site Scripting (XSS) vulnerabilities. Sophos UTM is a firewall solution by Sophos. It implements a web interface that allows authenticated users to manage quarantined mails. Additionally, users can inspect the contents of mails.

Sophos UTM failed to sanitize the following contents of mails before reflecting them within the web interface:

* subject

* filename(s) of attached file(s)

* sender's name

* mail body (actual contents)

Proof of Concept (PoC)

======================

1. Send an e-mail that purposely is sent to quarantine by Sophos UTM. This can be for instance achieved by including the "Generic Test for Unsolicited Bulk Email" (GTUBE) test string. Additionally, include the following markup:

```

<iframe src="asd">

<img src="x:gif" onerror="alert('asd')"></img>

```

2. Access the SMTP quarantine interface and display the detail view of the previously sent e-mail.

3. Observe that the XSS payload is executed within Sophos UTM's origin.

Credits

=======

This security vulnerability was found by Daniel Hoffmann of usd AG.

Please find the full advisory here:
<https://herolab.usd.de/security-advisories/usd-2020-0106/>
https://herolab.usd.de/security-advisories/usd-2020-0106/

In accordance with usd AG's Responsible Disclosure Policy (
<https://herolab.usd.de/en/responsible-disclosure/>
https://herolab.usd.de/en/responsible-disclosure/), all vendors have been notified of the existence of these vulnerabilities.

The information provided in these security advisories is provided "as is" and without warranty of any kind. Details of the security advisories at our

```
website may be updated in order to provide as accurate information as
possible.
```

Attachment: smime.p7s
Description:

```
_______________________________________________
Sent through the Full Disclosure mailing list
https://nmap.org/mailman/listinfo/fulldisclosure
Web Archives & RSS: http://seclists.org/fulldisclosure/
```

By Date   By Thread

Current thread:

- usd AG Security Advisories 11/2021 *Responsible Disclosure via Fulldisclosure (Dec 03)*

Site Search

Nmap Security Scanner

- Ref Guide
- Install Guide
- Docs
- Download
- Nmap OEM

Npcap packet capture

- User's Guide
- API docs
- Download
- Npcap OEM

Security Lists

- Nmap Announce
- Nmap Dev
- Full Disclosure
- Open Source Security
- BreachExchange

Security Tools

- Vuln scanners
- Password audit
- Web scanners
- Wireless
- Exploitation

About

- About/Contact
- Privacy
- Advertising
- Nmap Public Source License