SYNACKTIV
DIGITAL SECURITY

Multiple Stored Cross-Site Scripting vulnerabilities in Sage Enterprise Intelligence

Security advisory

21/12/2022

Antoine Gicquel
Mickaël Benassouli

Vulnerabilities description

Sage Enterprise Intelligence

Sage Enterprise Intelligence is an integrated BI software, helping users quickly take the best decisions, with every meaningful data they need.

With SEI, data is extracted, transformed, consolidated, migrated and displayed clearly, accessible live, in a few clicks.

The issues

Synacktiv has identified multiple vulnerabilities in Sage Enterprise Intelligence that allow an attacker to execute JavaScript code in the context of users' browsers. The attacker needs to be authenticated to reach the vulnerable features.

A vulnerability is present in the *Favorites* tab. The name of a favorite or a folder of favorites is interpreted as HTML, and can thus embed JavaScript code, which is executed when displayed. This is a self-XSS.

Another vulnerability is present in the *Notify Users About Modification* menu and the *Notifications* feature. A user can send malicious notifications and execute JavaScript code in the browser of every user having enabled notifications. This is a stored XSS, and can lead to privilege escalation in the context of the application.

Affected versions

At least the following version is affected. The previous versions have not been tested.

- 2021 R1.1

Timeline

Date	Action
07/06/2022	Advisory sent to Sage.
20/06/2022	Attribution of CVE ID: CVE-2022-34322
21/12/2022	Advisory published.

Technical description and Proof-of-Concept

Vulnerabilities discovery

Sage Enterprise Intelligence allows users to organize their favorites with folders. When creating a folder, the user is presented with the following pop-up:

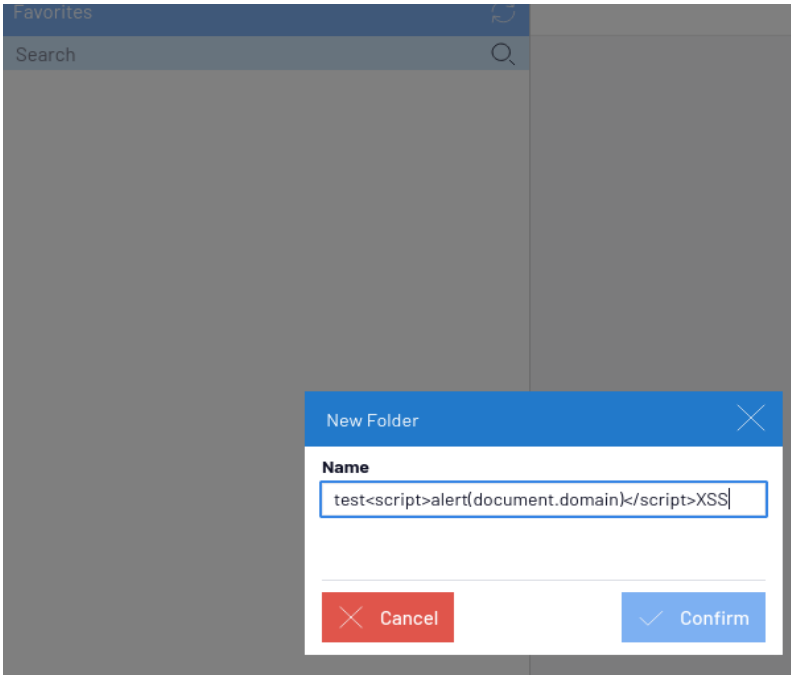

Illustration 1: Folder creation pop-up with a malicious name value

However, when injecting malicious HTML in the name input, the new folder is created and displayed, and the JavaScript is executed:

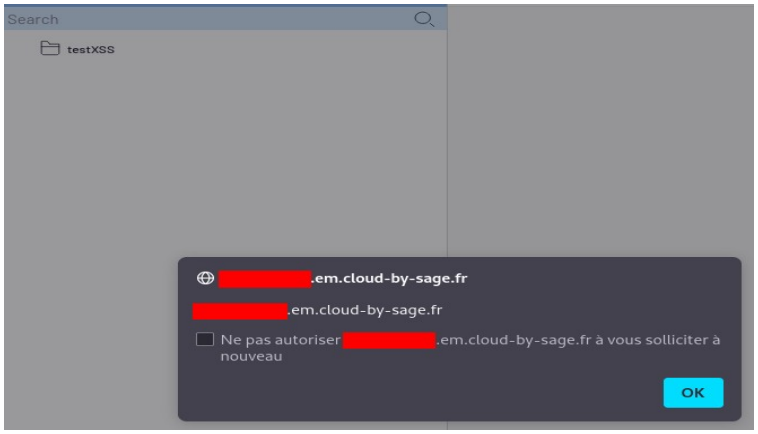

Illustration 2: Folder is created, displayed, and the JS is executed

Renaming favorites and favorites folders produces the same behavior.

Sage Enterprise Intelligence allows users to notify others about the modification of a document:

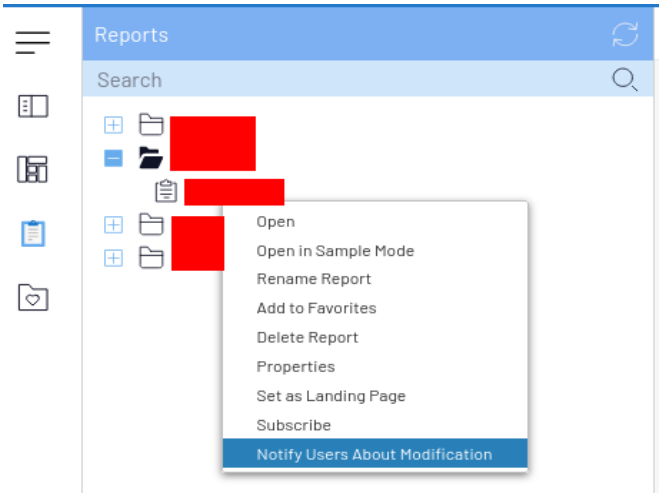

Illustration 3: Notify Users About Modification menu item appears when right-clicking an element in the tree.

When clicking this menu option, the following message is sent to the server via *SignalR*, an asynchronous web library from *Microsoft*:

```
{"H":"synchub","M":"SendNotification","A":["<img class='toolbarNotification-icon'
src='https://**********.em.cloud-by-sage.fr/Content/images/svg/ViewTypeGroups/
worksheet.svg'> <a href='#' class='viewLink'data-type='OpenView' data-
notiftype='ViewChange' data-processid='*********' data-id='*********'>
******************</a> has been modified by **************","","*PUBLIC"],"I":0}
```

The notification message, stored in the first element of the *A* array of the JSON payload, is then directly interpreted as HTML within the notification center, when displayed to users:

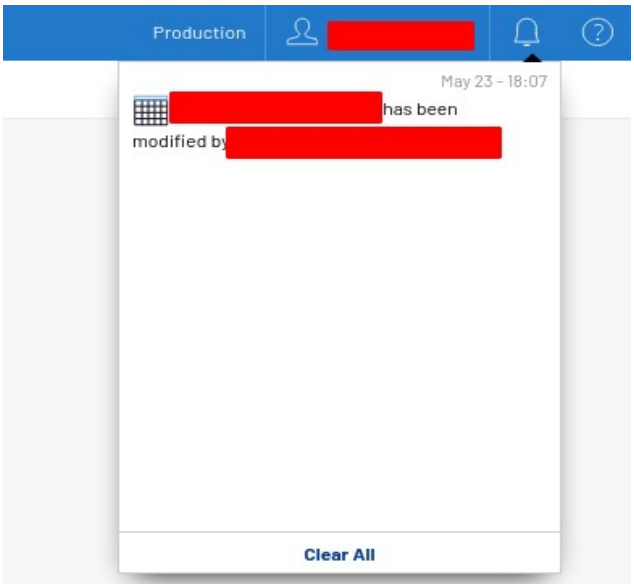

Illustration 4: Notification displayed by the other users

An attacker can send a malicious message to the server, containing a JavaScript payload. This payload will be executed by every user with notifications enabled, in real time or when they next log in.

```
{"H":"synchub","M":"SendNotification","A":["<script>alert(document.domain)</
script>","","*PUBLIC"],"I":0}
```

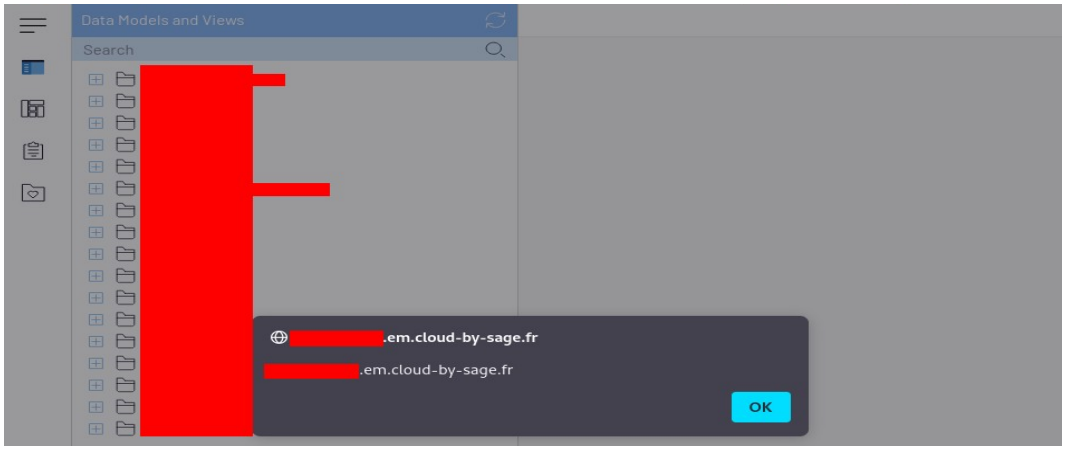

Illustration 5: The JavaScript payload is executed when the notification is received.

Impact

Depending on the cookies attributes, an authenticated attacker could either steal an administrator cookie or perform actions on the website on behalf of an administrator, such as adding a new user and granting them administrator privileges.