SiteVision Insufficient Module Access Control

CVE-2019-12734

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-12734

Summary

Attackers may inject non-authorised modules when editing pages using a low-privilege account, leading to impacts ranging from Cross-Site Scripting to Remote Code Execution.

Vendor Description

SiteVision AB is a Swedish product company focused on developing the portal and web publishing platform SiteVision.

Affected Versions

All versions of SiteVision 4 until 4.5.6.

All versions of SiteVision 5 until 5.1.1.

Earlier major versions are assumed to be vulnerable.

Technical Details

This vulnerability allows remote code execution as described in CVE-2019-12733.

Modules are basic building blocks in SiteVision pages and templates; they can feature display content such as headings and paragraphs, social functions and commenting, raw HTML, or server-side scripts.

The SiteVision application does not sufficiently assert whether or not the current user is authorised to add a specific module type to the current page, allowing attackers with low-privilege to add hostile content. This can trivially be reproduced by adding a paragraph text module, and changing "text" to "html" (or any other type) in the outgoing HTTP request. The application does not check whether or not the user is authorised to add the requested module; it relies on the fact that the user interface does not expose a button for it.

Reproduced on SiteVision 4 and 5; the following steps applies to SiteVision 5:

1. Install SiteVision and either create or import a new site.

2. Set up and create an Editor ("Redaktör") user.

3. Log on as the new low-privilege user.

4. Create a new page and note how only basic modules are available.

5. Insert a text module.

6. Re-send the HTTP request generated in step #5, but change the value of portletType from "text" to "html". The following is the resulting request for our demo environment:

```
POST /edit-api/1/4.549514a216b1c6180f41c3/4.549514a216b1c6180f41c3/portlet HTTP/1.1
Host: fast.furious
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:67.0) Gecko/20100101 Firefox/67.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en
Accept-Encoding: gzip, deflate
Referer: http://fast.furious/edit/4.549514a216b1c6180f41c3
Content-Type: application/json; charset=utf-8
X-CSRF-Token: [...]
X-Requested-With: XMLHttpRequest
Content-Length: 70
Connection: close
Cookie: [...]

{"portletType":"html","relativeElement":"12.549514a216b1c6180f41d0"}
```

7. Edit the HTML module and inject any JavaScript payload such as `<script>alert(1)</script>`.

8. Under "Other" check "Show in edit mode".

9. Press "OK".

10. Note the alert pop-up, indicating that the injected JavaScript was executed.

Vulnerability Disclosure Timeline

2019-06-03 - Disclosed to vendor

2019-06-04 - Vendor confirms vulnerability

2019-09-26 - Vendor issues patches

2019-12-04 - Public disclosure