Sitecore 10 Authenticated File upload to RCE / CVE-2021-38366

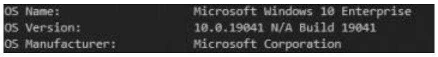
10/08/2021 Leave a comment Go to comments

After looking for some extreme hardening of the Sitecore client I found a way to get Remote Code execution (RCE) via a Update center, described in this post.

It is possible for authenticated users, to upload arbitrary files, via update package functionality.It is possible for a malicious attacker to bypass file upload restrictions, hardened with the Sitecore hardening guide https://doc.sitecore.com/en/developers/101/platform-administration-and-architecture/security-guide.html and with secure file upload functionality, taken from this link https://doc.sitecore.com/developers/100/platform-administration-and-architecture/en/secure-thefile-upload-functionality.html.

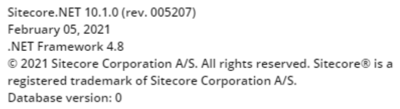
Test Instance information

The test of this was done on a local Windows 10 machine with Sitecore 10 XM installation, installed via Graphical installation wizard see more information below



```
OS Name:                   Microsoft Windows 10 Enterprise
OS Version:                10.0.19041 N/A Build 19041
OS Manufacturer:           Microsoft Corporation
```

System Information



Sitecore.NET 10.1.0 (rev. 005207)
February 05, 2021
.NET Framework 4.8
© 2021 Sitecore Corporation A/S. All rights reserved. Sitecore® is a registered trademark of Sitecore Corporation A/S.
Database version: 0

Sitecore version information

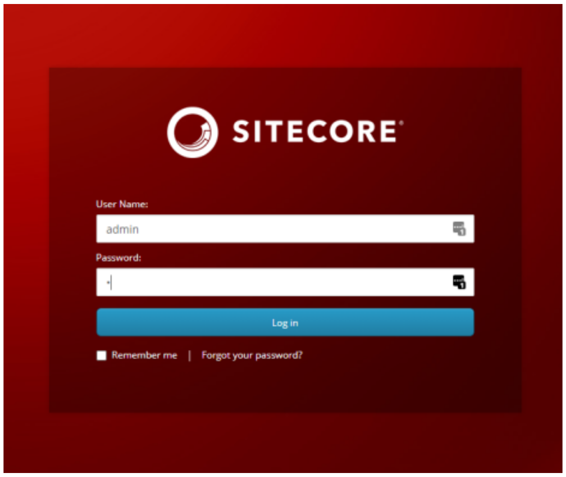
The Additional Filed upload restriction package was also installed with the following settings.

```
<?xml version="1.0" encoding="utf-8"?>
<configuration xmlns:patch="http://www.sitecore.net/xmlconfig/">
<sitecore>
<processors>
<uiUpload>
<processor mode="on"
type="Sitecore.Pipelines.Upload.CheckExtension,
Sitecore.UploadFilter" patch:before="*[1]">
<param desc="Allowed extensions (comma separated)"></param>
<param desc="Blocked extensions (comma separated)">exe,dll,aspx</param>
</processor>
</uiUpload>
</processors>
</sitecore>
</configuration>
```

Steps to reproduce

Keep in mind this is a autheticated file upload, so a compromised user must be obtained.

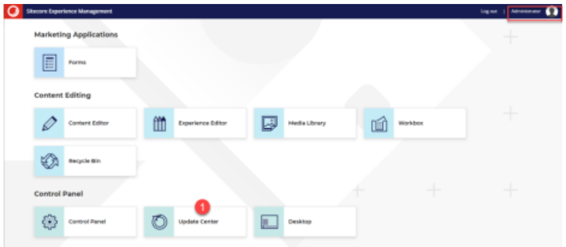
1. Authenticate / Login to Sitecore



2. Once correctly logged in. Navigate to the Upload center

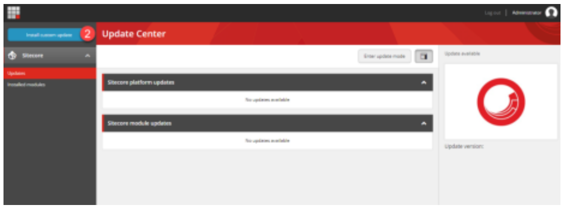
Privacy & Cookies: This site uses cookies. By continuing to use this website, you agree to their use.
To find out more, including how to control cookies, see here: Cookie Policy

Close and accept



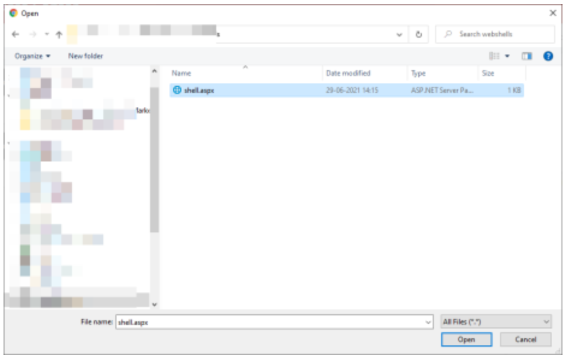
Navigated to update center

3. Choose/click the option to upload custom update



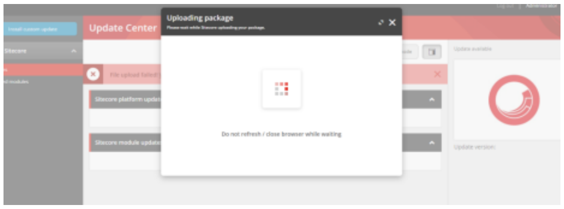
Upload via custom upload

4. Pick your custom webshell



Upload of custom webshell

5. If the installer hangs click anywhere in the windows, this is expected.


Install custom update
Update Center
Uploading package
Please wait while Sitecore uploading your package
Do not refresh / close browser while waiting
Sitecore platform updates
Sitecore module updates
Update available
Update version:

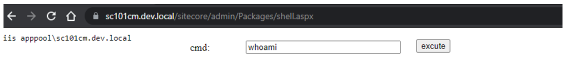
Uplaoder timesout / hangs

6. Since uploads of updates packages always goes into the same folder

https://HOSTNAME/sitecore/admin/Packages/

to find the uploaded file in our case
https://sc101cm.dev.local/sitecore/admin/Packages/shell.aspx

7. Now all that is left is running the webshell.



```
iis apppool\sc101cm.dev.local
```

cmd: whoami

Running our uploaded webshell

Remediation

Disabled the Update center functionality

One way of doing the in add restriction to path in web.config like below

```
 <location path="sitecore/api/ssc/updatecenter">
  <system.web>
      <authorization>
        <deny users="*" />
      </authorization>
    </system.web>
  </location>
```

Other

T
u

T
C

Privacy & Cookies: This site uses cookies. By continuing to use this website, you agree to their use.
To find out more, including how to control cookies, see here: Cookie Policy

Comments (2) Trackbacks (0) Leave a comment Trackback

1. Kenneth McAndrew (@kmac23va)
   10/08/2021 at 21:19
   Reply

   You say the remediation is to disable the update center. How do you go about doing this?

   - istern
     11/08/2021 at 09:17
     Reply

     Hi Kenneth
     Sorry somehow this part was missing, I've added in again, there might be better ways to do it but then one shown will limit all access to the updatecenter

1. No trackbacks yet.

Leave a Reply

Enter your comment here...

Obfuscating sensitive data in Azure Application Insights Should you trust your own website ?
RSS feed

Twitter

Recent Posts

- Obfuscating sensitive data in Azure Application Insights
- Sitecore 10 Authenticated File upload to RCE / CVE-2021-38366
- Should you trust your own website ?
- Sitecore 9.1 IdentityServer On-Premise AD via ADFS
- Sitecore installation Framework (SIF) custom install path.

Top Posts

- Sitecore 10 Authenticated File upload to RCE / CVE-2021-38366
- Obfuscating sensitive data in Azure Application Insights

Azure C# Code Kata CSS Docker Dropbox Elasticsearch Fakes Gallery Google HTML IdenityServer IIS IOC Java Javascript MongoDB MVC Ninject OAuth Rest Security Sitecore Solr TDD Umbraco Unit Testing Usability

Categories

- .Net
- Azure
- C#
- CSS
- Docker
- Elasticsearch
- Java
- Javascript
- Kibana
- Logstash
- MongoDB
- MVC
- Security
- Sitecore

Privacy & Cookies: This site uses cookies. By continuing to use this website, you agree to their use.
To find out more, including how to control cookies, see here: Cookie Policy

- Solr
- Uncategorized
- Unit Testing
- WFFM

My Recent Tweets

- RT @RealTryHackMe: Ho ho hackety ho! 🎅 To celebrate the launch of #AdventOfCyber, we’re giving away a limited edition #TryHackMe Yeti t-sh… 1 week ago
- RT @RealTryHackMe: Our brand new Red Teaming pathway is LIVE.🔥 Learn how to execute attack emulations as a Red Team Operator! We’re coinci… 3 months ago

Follow @T

Blogroll

- Briancaos
- Learn Sitecore
- Max S
- Molten Core

Archives

- May 2022
- August 2021
- February 2021
- May 2019
- February 2019
- November 2017
- April 2017
- February 2017
- November 2016
- October 2016
- September 2016
- December 2015
- November 2015
- March 2015
- January 2015
- October 2014
- June 2014
- May 2014
- November 2013
- October 2013
- September 2013
- June 2013
- April 2013
- October 2012
- September 2012
- July 2012
- May 2012
- April 2012
- February 2012
- November 2011
- October 2011
- July 2011
- June 2011
- May 2011
- December 2010
- November 2010
- June 2010
- April 2010
- March 2010
- February 2010
- January 2010
- November 2009
- October 2009
- July 2009
- June 2009
- May 2009

Meta

- Register
- Log in
- Entries feed
- Comments feed
- WordPress.com

Top
Blog at WordPress.com.

Privacy & Cookies: This site uses cookies. By continuing to use this website, you agree to their use.
To find out more, including how to control cookies, see here: Cookie Policy