MITIGATION INSTRUCTIONS

Mitigate your Orion Platform environment from the risk of the SUPERNOVA vulnerability using a new PowerShell script

solarwinds

Last Updated: Wednesday, December 23, 2020

SOLARWINDS DISCLAIMS ALL WARRANTIES, CONDITIONS, OR OTHER TERMS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, ON THE DOCUMENTATION, INCLUDING WITHOUT LIMITATION NONINFRINGEMENT, ACCURACY, COMPLETENESS, OR USEFULNESS OF ANY INFORMATION CONTAINED HEREIN. IN NO EVENT SHALL SOLARWINDS, ITS SUPPLIERS, NOR ITS LICENSORS BE LIABLE FOR ANY DAMAGES, WHETHER ARISING IN TORT, CONTRACT OR ANY OTHER LEGAL THEORY, EVEN IF SOLARWINDS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Table of Contents

Mitigate your Orion Platform environment from the risk of the SUPERNOVA vulnerability using a new PowerShell script

Summary

The following article describes how to use the new PowerShell script to correct the `web.config` file within your Orion Platform deployment to protect it against the Supernova vulnerability. For the latest details, including the list of affected Orion versions, please see the Security Advisory.

Overview

In response to the recent security vulnerability referred to as SUPERNOVA, SolarWinds has both provided:

- A new script that downloads and installs the URL Rewrite IIS extension from Microsoft (from https://www.iis.net/downloads/microsoft/url-rewrite) and then updates the `web.config` file within your Orion Platform deployment to protect against Remote Code Execution (RCE).
- A manual process which addresses the vulnerability.

Disclaimer

Scripts are not supported under any SolarWinds support program or service. Scripts are provided AS IS without warranty of any kind. SolarWinds further disclaims all warranties including, without limitation, any implied warranties of merchantability or of fitness for a particular purpose. The risk arising out of the use or performance of the scripts and documentation stays with you. In no event shall SolarWinds or anyone else involved in the creation, production, or delivery of the scripts be liable for any damages whatsoever (including, without limitation, damages for loss of business profits, business interruption, loss of business information, or other pecuniary loss) arising out of the use of or inability to use the scripts or documentation.

Environment

Apply this script to the Orion Main Poller, the main polling engine backup (HA Server), and all Orion additional Web Servers.

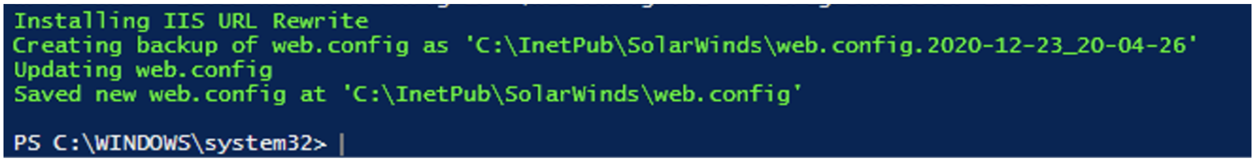
Using the Script

Execute the PowerShell script on your Orion server, any additional polling engines, HA servers, and websites that you want to check for the vulnerability.

1. Download the PowerShell script `Mitigate-TestAction.ps1`
2. Copy the script to the Orion Main Poller, the main polling engine backup (HA Server) and on each Orion additional website server.
3. As an administrator, execute the script in PowerShell.
4. Hashes:

Algorithm	Hash
SHA1	BA31CDC6DAE522008225899FF7C49E906A59BC1A
SHA256	FE0278A91A727A972AF49307F46762E2B1EEAAA7474BFE4FF81A676680BF5CF0
MD5	0BA63AA07D40A315F50B4879160065B5

You will see script output like the following:



```
Installing IIS URL Rewrite
Creating backup of web.config as 'C:\InetPub\SolarWinds\web.config.2020-12-23_20-04-26'
Updating web.config
Saved new web.config at 'C:\InetPub\SolarWinds\web.config'

PS C:\WINDOWS\system32> |
```

Manual Mitigation Instructions

Applying mitigation

These steps have to be executed on each Main Poller (MP), MB backup, and Additional Website (AW).

1. Download and install URL Rewrite IIS extension from https://www.iis.net/downloads/microsoft/url-rewrite

2. Locate root directory of Orion website:
    - Go to `C:\inetpub\SolarWinds`, or
    - Open IIS Manager, click on the "SolarWinds NetPerfMon" site in the left connections menu. Click on "Explore" in the actions menu on the right.
3. Open the `web.config` file for edit.
4. FIND the following line:

```
<defaultDocument enabled="true">
```

5. PASTE the following code BEFORE the above-mentioned line. Note that the rewrite section belongs under the `system.webserver` section:

```
<rewrite>
  <rules>
    <rule name="BLockInvalidAxdRequest" patternSyntax="ECMAScript"
stopProcessing="true">
        <match url="^[\s\S]+(Script|Web)Resource.axd" />
        <action type="CustomResponse" statusCode="403"
statusReason="Forbidden: Access is denied." statusDescription="You do not
have permission to view this directory or page using the credentials that
you supplied." />
    </rule>
    <rule name="PassValidi18nRequest" patternSyntax="ECMAScript"
stopProcessing="true">
        <match url="^[orion|webengine].*[css|js]\.i18n\.ashx$" />
        <conditions>
            <add input="{REQUEST_METHOD}" pattern="POST" negate="true" />
        </conditions>
        <action type="None" />
    </rule>
    <rule name="BLockOtheri18nRequest" patternSyntax="ECMAScript"
stopProcessing="true">
        <match url="i18n.ashx" />
        <action type="CustomResponse" statusCode="403"
statusReason="Forbidden: Access is denied." statusDescription="You do not
have permission to view this directory or page using the credentials that
you supplied." />
    </rule>
    <rule name="PassValidSkipi18nRequest" patternSyntax="ECMAScript"
```

```
stopProcessing="true">
        <match url="^Orion\/Skipi18n\/Profiler\/" />
        <action type="None" />
    </rule>
    <rule name="BLockOtherSkipi18nRequest" patternSyntax="ECMAScript"
stopProcessing="true">
        <match url="Skipi18n" />
        <action type="CustomResponse" statusCode="403"
statusReason="Forbidden: Access is denied." statusDescription="You do not
have permission to view this directory or page using the credentials that
you supplied." />
    </rule>
  </rules>
</rewrite>
```

6. Save the file.

Verification

1. Navigate in browser to `<YOUR_ORION_SERVER_NAME>/Orion/WebResource.axd`
2. You should receive `HTTP ERROR 403`

Reference

- URL Rewrite documentation - https://docs.microsoft.com/en-us/iis/extensions/url-rewrite-module/url-rewrite-module-configuration-reference
- Download URL Rewrite - https://www.iis.net/downloads/microsoft/url-rewrite