MITIGATION INSTRUCTIONS

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

solarwinds

Last Updated: Wednesday, January 13, 2021

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.

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 (© 2020 Microsoft, available at www.iis.net, obtained on December 30, 2020) 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.

ⓘ For the latest details about the vulnerability, including the list of affected Orion versions, please see the Security Advisory.

Environment

Orion Platform 2017.3, 2018.2, 2018.4, 2019.2, 2019.4, and 2020.2

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.

Using the script

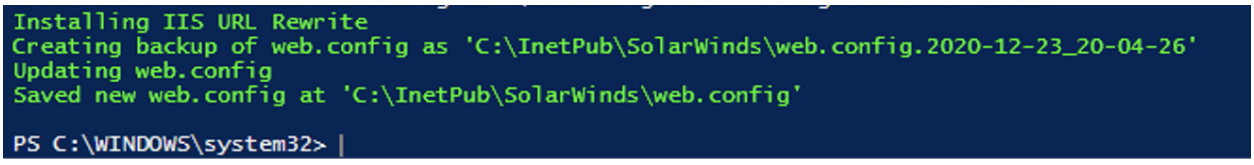
Execute the PowerShell script on your main Orion polling engine and all additional polling engines, high availability (HA) servers, and additional Web servers that you want to check for the vulnerability.

1. Download the PowerShell script `Mitigate-TestAction.ps1` from the following location: https://downloads.solarwinds.com/solarwinds/Support/SupernovaMitigation.zip.
2. Copy the script to your main Orion polling engine and all additional polling engines, HA servers, and additional Web servers.
3. As an administrator, execute the script in PowerShell.

Hashes:

Algorithm	Hash
SHA1	261B65E980D9FDD579A0D680697E7F9FF3CF3649
SHA256	D2AE8C5B844E1468EB980B37D2A89375EF762795B5021BE850E3B5E2CBEBB0CC
MD5	CB2321B4F87D06B8612A628611C4D008

You will see script output like the following:



Manual mitigation instructions

Applying mitigation

Execute these steps on your main Orion polling engine and all additional polling engines, high availability (HA) servers, and additional Web servers.

1. Download and install the URL Rewrite IIS extension from https://www.iis.net/downloads/microsoft/url-rewrite (© 2020 Microsoft, available at www.iis.net, obtained on December 30, 2020).
2. Locate the root directory of the Orion website:
   - Go to C:\inetpub\SolarWinds, or
   - Open IIS Manager, and click on the "SolarWinds NetPerfMon" site in the left connections menu. Then click on "Explore" in the actions menu on the right.
3. Open the `web.config` file for editing.
4. Look for the following line, and then perform one of the actions below:

   `<defaultDocument enabled="true">`

   - If you **do not** find the line, continue with step 5.
   - If you **do** find the line, 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>
```

5. If you did **not** find the line listed in step 4:

   a. Find the following line:

      `<system.webServer>`

   b. Press Enter to create a new line, and then paste the following code **after** 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 a 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 (© 2020 Microsoft, available at https://docs.microsoft.com/, obtained on December 30, 2020)
- Download URL Rewrite: https://www.iis.net/downloads/microsoft/url-rewrite (© 2020 Microsoft, available at www.iis.net, obtained on December 30, 2020)