TLP: WHITE

2019-125: Targeting of Microsoft SharePoint CVE-2019-0604

Version: 1, Last Updated: 6 May 2019

Overview

The Australian Cyber Security Centre (ACSC) is aware of malicious cyber actors successfully exploiting a Microsoft SharePoint vulnerability in order to implant web shells on compromised hosts.

This vulnerability (CVE-2019-0604) was originally identified in a security advisory published by Microsoft on 12 February 2019. This security advisory was subsequently updated on 25 April 2019 with a new software patch. This ACSC Advisory provides recommendations for securing Microsoft SharePoint and advice on identifying potential successful exploitation of this vulnerability.

Further details on this vulnerability are available from Microsoft[1].

Recommendations

Identify and patch vulnerable SharePoint servers

Organisations are strongly encouraged to apply the latest SharePoint patches available from Microsoft[2].

Investigate for evidence of exploitation

Organisations are strongly encouraged to engage their ICT team or provider and review their environments for evidence of the malicious activity outlined below.

Organisations should analyse SharePoint directories for any indications of the presence of web shells and other malicious files, particularly the `Layouts` folder. By default, the `Layouts` folder is located at the following path, depending on the SharePoint version:

```
C:\Program Files\Common Files\Microsoft Shared\Web Server
    Extensions\<version_number>\Template\Layouts
```

In order to identify potential web shells organisations should review and implement the guidance outlined in Detect and Prevent Web Shell Malware[3].

Organisations are also recommend to review web server logs, and other relevant sources of logging, for the following items which could indicate malicious activity associated with exploitation of this SharePoint vulnerable.

[1] Microsoft SharePoint Remote Code Execution Vulnerability: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0604
[2] Microsoft SharePoint Remote Code Execution Vulnerability: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0604
[3] cyber.gov.au Detect and Prevent Web Shell Malware: https://www.cyber.gov.au/advice/detect-and-prevent-web-shell-malware

Review HTTP POST requests to the following resources required to successfully exploit the CVE-2019-0604 vulnerability:

```
Picker.aspx?PickDialogType=Microsoft.SharePoint.WebControls.ItemPickerDialog

Picker.aspx?PickDialogType=Microsoft.SharePoint.Portal.WebControls.ItemPickerDialog
```

Implement complimentary security controls and/or transfer risk.

The ACSC strongly recommends the implementation of the ASD Essential 8 Mitigations[4] to mitigate threats to internet facing systems. Specifically for this vulnerability, maintaining a regular patch process and validating the application of patches reduces the risk of exploitation and is an essential part of a mature cyber program.

To limit the extent of cyber security incidents related to compromise of web servers, organisations should segment and segregate internet facing servers whenever possible. Methods of network segmentation for a web server may include:

- Move the web server to an appropriate network segment (e.g. a DMZ) for the environment
- Move the web application to an externally hosted server (e.g. within a cloud hosted environment)

The following controls should be applied to externally facing servers, whether DMZ or cloud based, to limit trust and data movement into the internal network. These controls will include:

- Apply host segregation by only allowing specified communications between servers where required and over specific protocols. Additional considerations and limitations should be applied to communications between the server and network internal segments.
- Internal authentication credentials should be protected from externally facing servers. Do not use or store internal segment credentials on externally facing servers.
- An additional protection for web servers is the removal of impersonate privileges from service accounts that do not require this privilege. *Please note: This will need testing as some service accounts may require this privilege.*

Additionally; logging on externally facing servers (both operating system and application logs) should capture the appropriate events to enable a security team to effectively monitor for compromise. The logs should be centralised and continuously monitored for signs of anomalous activity.

Incident Reporting

If you have questions about this advice or have indications that your environment has been compromised, contact the ACSC by emailing **asd.assist@defence.gov.au** or calling **1300 CYBER1 (1300 292 371)**.

[4] cyber.gov.au Essential Eight Explained: https://www.cyber.gov.au/publications/essential-eight-explained

Traffic Light Protocol

The Traffic Light Protocol utilised by the ACSC is defined by the Forum of Incident Response and Security Teams, Inc. (FIRST). A complete version of the FIRST TLP Standards Definitions and Usage Guidance is available from FIRST[5].

TLP Level	Restriction on access and use
RED	**Not for disclosure, restricted to participants only.** Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused. Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
AMBER	**Limited disclosure, restricted to participant's organisations..** Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organisations involved. Recipients may only share TLP:AMBER information with members of their own organisation, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**
GREEN	**Limited disclosure, restricted to the community.** Sources may use TLP:GREEN when information is useful for the awareness of all participating organisations as well as with peers within the broader community or sector. Recipients may share TLP:GREEN information with peers and partner organisations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not released outside of the community.
WHITE	**Disclosure is not limited.** Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.
Not classified	Any information received from the ACSC that is not classified in accordance with the Traffic light protocol must be treated as AMBER classified unless otherwise agreed in writing by the ACSC.

[5] FIRST Traffic Light Protocol Standards Definitions and Usage Guidance: https://www.first.org/tlp/