National Cyber Security Centre
a part of GCHQ

Alert: Risk of SharePoint vulnerability CVE-2020-16952 to UK organisations

Version 1.0

16 October 2020

Introduction

The NCSC is raising awareness of a new remote code execution vulnerability (CVE-2020-16952) affecting Microsoft SharePoint. Successful exploitation of this vulnerability would allow an attacker to run arbitrary code and carry out security actions in the context of the local administrator on affected installations of SharePoint server.

The NCSC always recommends applying security updates promptly to mitigate the exploitation of **all** vulnerabilities but in this case the NCSC has previously seen a large number of exploitations of SharePoint vulnerabilities, such as CVE-2019-0604, against UK organisations. Two SharePoint CVEs also appear in the CISA Top 10 Routinely Exploited Vulnerabilities.

The NCSC is issuing this alert to ensure that system owners are aware of this vulnerability and to ensure remediation actions are taken.

Details

The vulnerability is a caused by a validation issue in user-supplied data.[1] This vulnerability can be exploited when a user uploads a specially crafted SharePoint application package to an affected version of SharePoint. This affects versions:

- Microsoft SharePoint Foundation 2013 Service Pack 1
- Microsoft SharePoint Enterprise Server 2016
- Microsoft SharePoint Server 2019

SharePoint Online as part of Office 365 is not affected.

The October 2020 SharePoint security update addresses the vulnerability by correcting how SharePoint checks the source markup of application packages.

Further information on how the vulnerability works can be found here.

Mitigation

This vulnerability can be mitigated by ensuring that the relevant security updates are installed. Microsoft has published an advisory on this vulnerability which includes links to these updates:

https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2020-16952

[1] More information from the researcher who discovered the vulnerability is available here: https://srcincite.io/advisories/src-2020-0022/

Detection

Proof of concept code (PoC) is available here.

This PoC can be detected by identifying HTTP headers containing the string runat="server", as well as auditing SharePoint page creations.

Conclusion

The NCSC **strongly advises** that organisations refer to the Microsoft guidance referenced in this alert and ensure the necessary updates are installed in affected SharePoint products. It is also important to keep informed of any possible updated future updates to the guidance via this link.

The NCSC generally recommends following vendor best practice advice in the mitigation of vulnerabilities. In the case of this SharePoint vulnerability, it is important to install the latest updates as soon as practicable.

Mitigation

A variety of mitigations will be useful in defending against the campaigns detailed in this report:

- **Protect your devices and networks by keeping them up to date**: use the latest supported versions, apply security updates promptly, use anti-virus and scan regularly to guard against known malware threats. See NCSC Guidance: https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks.
- **Prevent and detect lateral movement in your organisation's networks**. See NCSC Guidance: https://www.ncsc.gov.uk/guidance/preventing-lateral-movement.
- **Set up a security monitoring capability** so you are collecting the data that will be needed to analyse network intrusions. See NCSC Guidance: https://www.ncsc.gov.uk/guidance/introduction-logging-security-purposes.
- **Review and refresh your incident management processes.** See NCSC Guidance: https://www.ncsc.gov.uk/collection/incident-management.
- **Further information:** Invest in preventing malware-based attacks across various scenarios. See NCSC Guidance: https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks