National Cyber Security Centre
a part of GCHQ

# Alert: Exploitation of CVE-2019-0604 Microsoft SharePoint Remote Code Vulnerability

Version 1.0

Reference: NCSC-Ops/15-19

16 May 2019

## About this document

This report provides information derived from NCSC and industry analysis on a recent trend of attacks against a Microsoft SharePoint Remote Code Execution Vulnerability CVE-2019-0604. It includes information to help with detection and mitigation advice.

## Disclaimer

This report draws on information derived from NCSC and industry sources. Any NCSC findings and recommendations made have not been provided with the intention of avoiding all risks, and following the recommendations will not remove all such risk. Ownership of information risks remains with the relevant system owner at all times.

## Introduction

A remote code execution vulnerability (CVE-2019-0604) exists in various Microsoft SharePoint versions. Microsoft have published information and guidance, as well as providing a patch to address the vulnerability.

The NCSC have continued to see a high level of successful attacks using this vulnerability as an initial attack vector against UK organisations. The NCSC are issuing this alert to ensure that system owners are aware of this vulnerability and to check that remediation actions have been taken.

## Details

The vulnerability covered under CVE-2019-0604 allows an attacker to run arbitrary code by uploading a specifically crafted SharePoint application package to vulnerable versions of SharePoint.

For more specific information about this vulnerability, please see the Microsoft article at the following address:

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0604

Microsoft have released a patch for this vulnerability for the following versions of SharePoint:

Microsoft SharePoint Enterprise Server 2016
Microsoft SharePoint Foundation 2010 Service Pack 2
Microsoft SharePoint Foundation 2013 Service Pack 1
Microsoft SharePoint Server 2010 Service Pack 2
Microsoft SharePoint Server 2013 Service Pack 1
Microsoft SharePoint Server 2019

A snort signature also exists to detect exploitation against this vulnerability (Snort ID 49681). Further information about this can be found on the Snort website:

https://snort.org/rule_docs/1-49861

## Conclusion

Successful exploitation of this vulnerability could allow an attacker to gain access to sensitive data, enable lateral movement within a network and potentially use the access to target an organisation's customers and suppliers.

If you believe that your organisation has been a victim of this vulnerability, please report this to the NCSC.

## Mitigation

Network defenders are advised to follow these mitigation points to protect their organisations against exploitation of this vulnerability:

- **Protect your devices and networks by keeping them up to date**: use the latest supported versions, apply security patches promptly, use anti-virus and scan regularly to guard against known malware threats. See NCSC Guidance: https://www.ncsc.gov.uk/guidance/mitigating-malware.
- **Restrict intruders' ability to move freely around your systems and networks.** Pay particular attention to potentially vulnerable entry points eg third-party systems with onward access to your core network. During an incident, disable remote access from third-party systems until you are sure they are clean. See NCSC Guidance: https://www.ncsc.gov.uk/guidance/preventing-lateral-movement and https://www.ncsc.gov.uk/guidance/assessing-supply-chain-security.
- **Review and refresh your incident management processes.** See NCSC Guidance: https://www.ncsc.gov.uk/guidance/10-steps-incident-management.