UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00186

MICROSOFT RACES TO FIX EOP FLAW

DATE ISSUED: 23rd August 2021

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

After confirming with Microsoft that the flaw would not be fixed, Google's Project Zero released information regarding an Elevation of Privilege flaw in regard to AppContainers which has prompted Microsoft to race to remediate the issue after more information has come to light.

BREAKDOWN

Normally, researchers must wait for a period of 90days before disclosing any discovered flaws unless the vendor expresses that they will not be fixing the bug, then the information may be released to the public. In this case, Microsoft reneged the Won'tFix status of the flaw in AppContainers which may allow an attacker to escalate their privileges by exploiting the default Windows Filtering Platform (WFP) rules. The flaw within the WFP set of APIs and system services (providing a platform for creating network filtering apps – in other words allow executable files to connect to TCP sockets in AppContainers) means that an attacker may connect to an AppContainer and inject malicious code. Initially, Microsoft believed a compromised AppContainer would be required to perform the attack, making it a non-issue but it has since come to light that remote connection is possible.

REMEDIATION STEPS

- Check connection rules to AppContainers are not "too flexible" and remediate where necessary – more information provided in the resources below.
- Update to the latest Windows 10 version and apply security updates as soon as they become available.

REFERENCES & RESOURCES

Threatpost https://threatpost.com/windows-eop-bug-detailed-by-google-project-zero/168823/
Google Project Zero https://googleprojectzero.blogspot.com/2021/08/understanding-network-access-windows-app.html