McAfee Enterprise Defender Blog | MSHTML CVE-2021-40444

By Taylor Mullins, Ben Marandel and Mo Cashman on Sep 20, 2021

Threat Summary

Microsoft is warning its users of a zero-day vulnerability in Windows 10 and versions of Windows Server that is being leveraged by remote, unauthenticated attackers to execute code on the target system using specifically crafted office documents. Tracked as CVE-2021-40444 (CVSS score: 8.8), the remote code execution flaw is rooted in MSHTML (aka Trident), a proprietary browser engine for the now-discontinued Internet Explorer and which is used in Microsoft Office to render web content inside Word, Excel, and PowerPoint documents. This vulnerability is being actively exploited and protections should be put into place to prevent that. Microsoft has released guidance on a workaround, as well as updates to prevent exploitation, but below are additional McAfee Enterprise countermeasures you can use to protect your business.

MVISION Insights Campaign – “CVE-2021-40444 – Microsoft MSHTML Remote Code Execution Vulnerability”

Since originally reported, vulnerability exploitation has grown worldwide.

Figure 1. Latest MITRE ATT&CK framework for Exploitation of CVE-2021-40444. Source: MVISION Insights

Additional MITRE ATT&CK techniques have been identified since our original report. MVISION Insights will be regularly updated with the latest IOCs and hunting rules for proactive detection in your environment.

Figure 2. Latest MITRE ATT&CK framework for Exploitation of CVE-2021-40444. Source: MVISION Insights

McAfee Enterprise Product Protections

The following McAfee Enterprise products can protect you against this threat.

Figure 3. Protection by ENS Module

For ENS, it's important to have both Threat Protection (TP) and Adaptive Threat Protection (ATP) with GTI enabled. We are seeing 50% of detections based on ATP behavior analysis rules.

Figure 4. Protection by ENS Module

More details on Endpoint protection including MVISION EDR are included below.

Preventing Exploit with McAfee ENS

McAfee Global Threat Intelligence (GTI) is currently detecting the analyzed IOCs for this exploitation. GTI will be continually updated as new indicators are observed in the wild.

ENS Threat Prevention module can provide added protections against exploitation of CVE-2021-40444 until a patch is deployed. The following signature in Exploit Prevention has shown coverage in testing of observed exploits; this signature could cause false positives, so it is highly advised to test in Report Mode or in sandbox environments before blocking in production environments.

Signature 2844: Microsoft Word WordPerfect5 Converter Module Buffer Overflow Vulnerability

Several custom **Expert Rules** can be implemented to prevent or detect potential exploitation attempts. As with all Expert Rules, please test them in your environment before deploying widely to all endpoints. Recommended to implement this rule in a log only mode to start.

Figure 5. Expert Rule to block or log exploitation attempts

Figure 6. Expert Rule to block or log exploitation attempts

ATP Rules

Adaptive Threat Protection module provides behavior-blocking capability through threat intelligence, rules destined to detect abnormal application activity or system changes and cloud-based machine-learning. To exploit this vulnerability, the attacker must gain access to a vulnerable system, most likely through Spearphishing with malicious attachments. These rules may also be effective in preventing initial access and execution. It is recommended to have the following rules in Observe mode at least and monitor for threat events in ePO.

- Rule 2: Use Enterprise Reputations to identify malicious files.
- Rule 4: Use GTI file reputation to identify trusted or malicious files
- Rule 5: Use GTI file reputation to identify trusted or malicious URLs
- Rule 300: Prevent office applications from being abused to deliver malicious payloads
- Rule 309: Prevent office applications from being abused to deliver malicious payloads
- Rule 312: Prevent email applications from spawning potentially malicious tools

As with all ATP Rules, please test them in your environment before deploying widely to all endpoints or turning on blocking mode.

Utilizing MVISION EDR for Hunting of Threat Activity

The Real-Time Search feature in MVISION EDR provides the ability to search across your environment for behavior associated with the exploitation of this Microsoft vulnerability. Please see the queries to locate the “mshtml” loaded module associated with various application processes.

EDR Query One

Processes where Processes parentimagepath matches “winword|excel|powerpnt” and Processes cmdline matches “AppData\/Local\/Temp\/|\.inf|\.dll” and Processes imagepath ends with “\control.exe”

EDR Query Two

HostInfo hostname and LoadedModules where LoadedModules process_name matches “winword|excel|powerpnt” and LoadedModules module_name contains “mshtml” and LoadedModules module_name contains “urlmon” and LoadedModules module_name contains “wininet**“**

Additionally, the Historical Search feature within MVISION EDR will allow for the searching of IOCs even if a system is currently offline.

Figure 7. Using Historical Search to locate IOCs across all devices. Source: MVISION EDR

McAfee Enterprise has published the following KB article that will be updated as more information and coverage is released.

McAfee Enterprise coverage for CVE-2021-40444 – MSHTML Remote Code Execution

Further Protection for Threat Actor Behavior After Exploitation

Since public disclosure of the vulnerability, it has been observed from successful exploitation of CVE-2021-40444 in the wild that threat actors are utilizing a Cobalt Strike payload to then drop ransomware later in the compromised environment. The association between this vulnerability and ransomware point to the possibility that the exploit has been added to the tools utilized in the ransomware-as-a-service (RaaS) ecosystem.

Figure 8. CVE-2021-40444-attack-chain (Microsoft)

The Ransomware Gangs that have been observed in these attacks have in the past been known to utilize the Ryuk and Conti variants of ransomware.

Please see below additional mitigations that can be utilized in the event your environment is compromised and added protections are needed to prevent further TTPs.

Cobalt Strike BEACON

MVISION Insights Campaign – Threat Profile: CobaltStrike C2s

Endpoint Security – Advanced Threat Protection:

Rule 2: Use Enterprise Reputations to identify malicious files.

Rule 4: Use GTI file reputation to identify trusted or malicious files

Rule 517: Prevent actor process with unknown reputations from launching processes in common system folders

Ryuk Ransomware Protection

MVISION Insights Campaign – Threat Profile: Ryuk Ransomware

Endpoint Security – Advanced Threat Protection:

Rule 2: Use Enterprise Reputations to identify malicious files.

Rule 4: Use GTI file reputation to identify trusted or malicious files

Rule 5: Use GTI file reputation to identify trusted or malicious URLs

Endpoint Security – Access Protection:

Rule: 1

Executables (Include):

*

Subrules:

Subrule Type: Files

Operations:

Create

Targets (Include):

*.ryk

Endpoint Security – Exploit Prevention

Signature 6153: Malware Behavior: Ryuk Ransomware activity detected

Conti Ransomware Protection

MVISION Insights Campaign – Threat Profile: Conti Ransomware

Endpoint Security – Advanced Threat Protection:

Rule 2: Use Enterprise Reputations to identify malicious files.

Rule 4: Use GTI file reputation to identify trusted or malicious files

Rule 5: Use GTI file reputation to identify trusted or malicious URLs

Endpoint Security – Access Protection Custom Rules:

Rule: 1

Executables (Include):

*

Subrules:

Subrule Type: Files

Operations:

create

Targets (Include):

*conti_readme.txt

Endpoint Security – Exploit Prevention

Signature 344: New Startup Program Creation

About the Author

Taylor Mullins

Taylor Mullins regularly advises our global customers in the areas of cyber threat management, threat intelligence, and their device-to-cloud data protection strategy. Taylor has been in the security space for five years and IT technology for over twenty years. Outside of work Taylor enjoys cycling, baseball, and spending time with his family.

Read more posts from Taylor Mullins ›

Ben Marandel

Ben is one of McAfee's passionate engineers in cybersecurity. He recently appointed Solution Architect for the EMEA region and was previously Endpoint Specialist for South Europe. He's specialized in building enterprise architecture designs to help enterprises fighting new cyber threats with tools such as EPP, EDR/XDR, Threat Intel and Automation. With that passion and over ...

Read more posts from Ben Marandel ›

Mo Cashman

Mo Cashman is one of the company's passionate leaders in cyber security. As an Enterprise Security Architect and Principal Engineer at McAfee, Mo advises our largest global customers and partners on their cyber threat management and data protection strategies for the digital enterprise. Mo's passion is to inspire our next generation security professionals as well ...

Read more posts from Mo Cashman ›

‹ Previous Article

Next Article ›

Categories: McAfee Enterprise

Subscribe to McAfee Securing Tomorrow Blogs

Email address

Subscribe

New to McAfee Enterprise?

What Is MVISION?
Cloud Security Products
Endpoint Protection Products
Explore Products
Explore Services
Skyhigh
Skyhigh Networks

About McAfee Enterprise

About Us
Latest News
Diversity & Inclusion
Careers
Blogs

Resources

Enterprise Support
Product Downloads
Product Documentation
Shop Online
Renew Products
Partner Portal Login
Free Trials
Free Tools

Connect with Us

Contact Us
Find a Partner
Partners
MPOWER
Events
Webinars

United States / English

Privacy | Legal Notices | Legal Contracts & Terms | Site Map |