The Bug Report | September 2021: CVE-2021-40444

By Kevin McGrath, Eoin Carroll and Steve Povolny on Sep 17, 2021

Why am I here?

There's a lot of information out there on critical vulnerabilities; this short bug report contains an overview of what we believe to be the most news and noteworthy vulnerabilities. We don't rely on a single scoring system like CVSS to determine what you need to know about; this is all about qualitative and experience-based analysis, relying on over 100 years of combined industry experience within our team. We look at characteristics such as wormability, ubiquity of the target, likelihood of exploitation and impact. Today, we'll be focusing on CVE-2021-40444.

CrossView: CVE-2021-40444

What is it?

CVE-2021-40444 is a vulnerability in Office applications which use protected view such as Word, PowerPoint and Excel which allows an attacker to achieve remote code execution (RCE). CVE-2021-40444 is a vulnerability which allows a carefully crafted ActiveX control and a malicious MS Cabinet (.cab) file to be launched from an Office document.

Most importantly, this vulnerability impacts the applications themselves, as well as the Windows Explorer preview pane.

Who cares?

This is a great question! Pretty much anyone who uses any Microsoft Office applications, or has them installed, should be concerned.

Office is one of the most widely-used applications on the planet. Odds are good you have it open right now. While many companies have disabled macros within Office documents at the Group Policy level, it is unlikely ActiveX is treated similarly. This means that without proper data hygiene, a large proportion of Office users will be vulnerable to this exploit.

Fortunately, "spray and pray" style email campaigns are unlikely to gain traction with this exploit, as mail providers have started flagging malicious files (or at least known PoCs) as potential malware and removing them as attachments.

What can I do?

Good news! You aren't necessarily completely helpless. By default, Windows uses a flag known as the "Mark of the Web" (MoTW) to enable Protected Mode in Office. Email attachments, web downloads, and similar all have this MoTW flag set, and Protected Mode prevents network operations, ActiveX controls, and macros embedded within a document from being executed, which effectively disables exploitation attempts for this vulnerability.

That said, users have become so inured to the Protected View message, they often dismiss it without considering the consequences. Much like "confirmation fatigue" can lead to installing malicious software, attackers can leverage this common human response to compromise the target machine.

Even more so, while exploitation can occur via the Office applications themselves and via the Explorer preview pane, the Outlook preview pane operates in a completely different manner which does not trigger the exploit. Exactly why this distinction exists only MS can explain, but the upshot is that Outlook users have to explicitly open malicious files to be exploited – the more hoops users have to jump through to open a malicious, the less likely they are to be pwned.

If I'm protected by default, why does this matter?

It depends entirely on how the file gets delivered and where the user saves it.

There are many ways of getting files beyond email and web downloads – flash cards for cameras, thumb drives, external hard drives, etc. Files opened from these sources (and many common applications[1]) don't have MoTW flag set, meaning that attackers could bypass the protection entirely by sending a malicious file in a .7z archive, or as part of a disk image, or dropping a USB flash drive in your driveway. Convincing users to open such files is no harder than any other social engineering strategy, after all.

Another fun workaround for bypassing default protections is to make use of an RTF file – emailed, downloaded, or otherwise. From our testing, an RTF file saved from an email attachment does not bear the MoTW but can still be used as a vector of exploitation. Whether RTF files become the preferred option for this exploit remains to be seen.

TL;DR

Ha! We put the tl;dr near the end, which only makes sense when the information above is so important it's worth reading. But if all you care about is what you can actively do to ensure you're not vulnerable, this section is for you.

Mitigations:

- Apply the Patch! Available via Windows Update as of 9/14/2021, this is your best solution.
- Enable registry workaround to disable ActiveX – details can be found on Microsoft's bulletin page and should effectively disable exploitation attempts until a formal patch can be applied.
- Confirm that Windows Explorer "Preview" pane is disabled (this is true by default). This only protects against the Preview pane exploitation in Explorer. Opening the file outside of Protected Mode (such as an RTF file) or explicitly disabling Protected Mode will still allow for exploitation.

The Gold Standard

In case you simply can't apply the patch or have a "production patch cycle" or whatever, McAfee Enterprise has you covered. Per our KB we provide comprehensive coverage for this attack across our protection and detection technology stack of endpoint (ENS Expert Rules), network (NSP) and EDR.

https://kc.mcafee.com/corporate/index?page=content&id=KB94876

[1] 7zip, files from disk images or other container formats, FAT formatted volumes, etc.

About the Author

Kevin McGrath

D. Kevin McGrath is a Security Researcher on McAfee's Advanced Threat Research team, focused on finding new vulnerabilities in both software and hardware. Kevin has a focus on embedded devices, RTOS security, and security education, with emphasis on computer architecture and operating systems.

Read more posts from Kevin McGrath ›

Eoin Carroll

Eoin Carroll is a Principal Engineer and Senior Vulnerability Researcher on the McAfee Advanced Threat Research team, focused on researching the trustworthiness of emerging computing platforms and protocols. He also analyzes critical industry vulnerabilities and innovates advanced threat defenses. He has 20 years of diverse experience, from electronic engineering to a variety of offensive and ...

Read more posts from Eoin Carroll ›

Steve Povolny

Steve Povolny is the Head of Advanced Threat Research for McAfee Enterprise, which delivers groundbreaking vulnerability research spanning nearly every industry. With more than a decade of experience in network security, Steve is a recognized authority on hardware and software vulnerabilities, and regularly collaborates with influencers in academia, government, law enforcement, consumers and enterprise businesses ...

Read more posts from Steve Povolny ›

‹ Previous Article

Categories: McAfee Enterprise ATR

Email address

Subscribe

Securing Tomorrow

New to McAfee Enterprise?

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

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

About McAfee Enterprise

About Us
Latest News
Diversity & Inclusion
Careers
Blogs

United States / English

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