1-Click Hack Found in Popular Desktop Apps — Check If You're Using Them

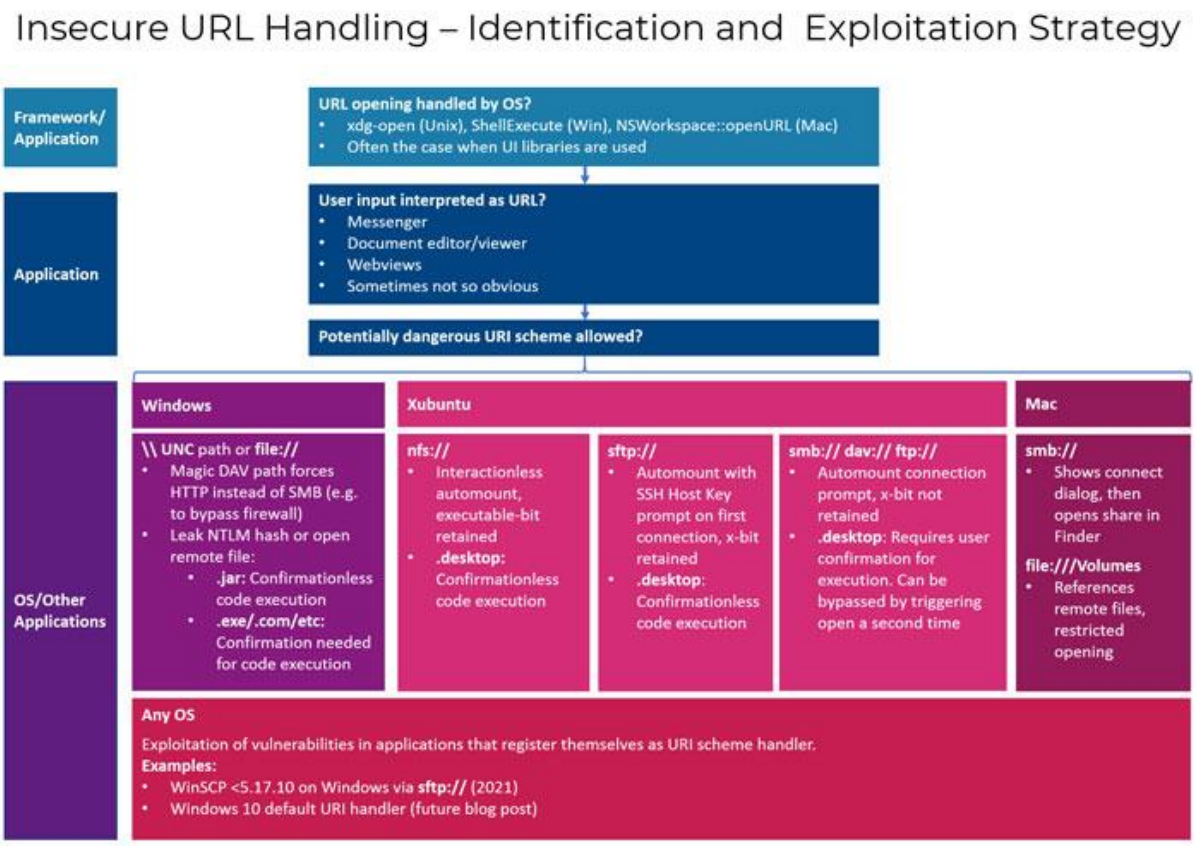
Multiple one-click vulnerabilities have been discovered across a variety of popular software applications, allowing an attacker to potentially execute arbitrary code on target systems.

The issues were discovered by Positive Security researchers Fabian Bräunlein and Lukas Euler and affect apps like Telegram, Nextcloud, VLC, LibreOffice, OpenOffice, Bitcoin/Dogecoin Wallets, Wireshark, and Mumble.

"Desktop applications which pass user supplied URLs to be opened by the operating system are frequently vulnerable to code execution with user interaction," the researchers said. "Code execution can be achieved either when a URL pointing to a malicious executable (.desktop, .jar, .exe, …) hosted on an internet accessible file share (nfs, webdav, smb, …) is opened, or an additional vulnerability in the opened application's URI handler is exploited."

Put differently; the flaws stem from an insufficient validation of URL input that, when opened with the help of the underlying operating system, leads to inadvertent execution of a malicious file.

Positive Security's analysis found that many apps failed to validate the URLs, thereby allowing an adversary to craft a specially-crafted link pointing to a piece of attack code, resulting in remote code execution.



Following responsible disclosure, most of the apps have released patches to remediate the flaws:

- Nextcloud - Fixed in version 3.1.3 of Desktop Client released on February 24 (CVE-2021-22879)
- Telegram - Issue reported on January 11 and subsequently fixed via a server-side change on (or slightly before) February 10
- VLC Player - Issue reported on January 18, with patched version 3.0.13 set for release next week
- OpenOffice - To be fixed in the upcoming (CVE-2021-30245)
- LibreOffice - Addressed in Windows, but vulnerable in Xubuntu (CVE-2021-25631)
- Mumble - Fixed in version 1.3.4 released on February 10 (CVE-2021-27229)
- Dogecoin - Fixed in version 1.14.3 released on February 28

- Bitcoin ABC - Fixed in version 0.22.15 released on March 9
- Bitcoin Cash - Fixed in version 23.0.0 (currently in release process)
- Wireshark - Fixed in version 3.4.4 released on March 10 (CVE-2021-22191)
- WinSCP - Fixed in version 5.17.10 released on January 26 (CVE-2021-3331)

"This issue spans multiple layers in the targeted system's application stack, therefore making it easy for the maintainers of any one to shift the blame and avoid taking on the burden of implementing mitigation measures on their end," the researchers said.

"However, due to the diversity of client systems and their configuration states, it is crucial that every party involved takes on some amount of responsibility and adds their contribution in the form of mitigation measures" such as URL validation and preventing remote shares from being auto-mounted.

Recommendations:

1. NEVER EVER give anyone your password. Doesn't matter who asks or why.
2. Avoid opening unsolicited attachments.
3. Be wary of social engineering.
4. Don't blindly click links.
5. If you do click an unsolicited link, and it takes you to a sign-in page, DON'T sign in.
6. Ensure Security of your Personal Information.
7. Enter personal information only on secure website.
8. Delete suspicious email and do not click.
9. Never provide your personal Information.
10. Check the correctness of email addresses.
11. Arrange Cyber security training and awareness workshop

References:

- https://thehackernews.com/2021/04/1-click-hack-found-in-popular-desktop.html
- https://www.jioforme.com/one-click-hacks-found-in-popular-desktop-apps-see-if-youre-using-them/343357/
- https://thecybersecurity.news/general-cyber-security-news/1-click-hack-found-in-popular-desktop-apps-check-if-youre-using-them-8181/
- https://hotforsecurity.bitdefender.com/blog/one-click-remote-code-execution-vulnerabilities-found-in-multiple-popular-apps-25674.html