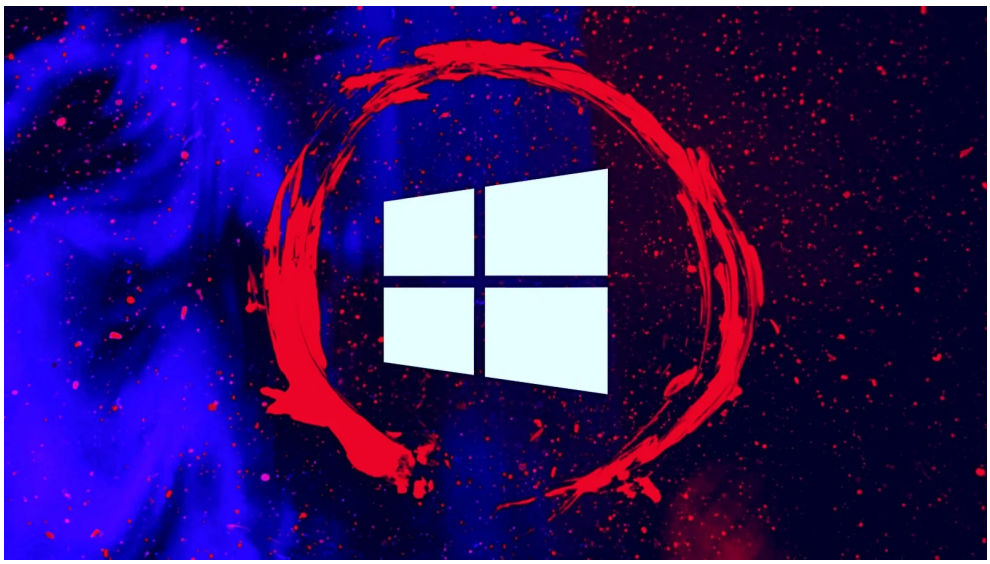
Windows vulnerability with new public exploits lets you become admin

By **Lawrence Abrams (https://www.bleepingcomputer.com/author/lawrence-abrams/)**

January 29, 2022 02:06 PM **3**



A security researcher has publicly disclosed an exploit for a Windows local privilege elevation vulnerability that allows anyone to gain admin privileges in Windows 10.

Using this vulnerability, threat actors with limited access to a compromised device can easily elevate their privileges to help spread laterally within the network, create new administrative users, or perform privileged commands.

The vulnerability affects all supported support versions of Windows 10 before the January 2022 Patch Tuesday updates.

Researcher releases bypass to patched vulnerability

As part of the January 2022 Patch Tuesday, Microsoft fixed a 'Win32k Elevation of Privilege Vulnerability' vulnerability tracked as CVE-2022-21882 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21882), which is a bypass for the previously patched and actively exploited CVE-2021-1732 bug (https://www.bleepingcomputer.com/news/security/recently-fixed-windows-zero-day-actively-exploited-since-mid-2020/).

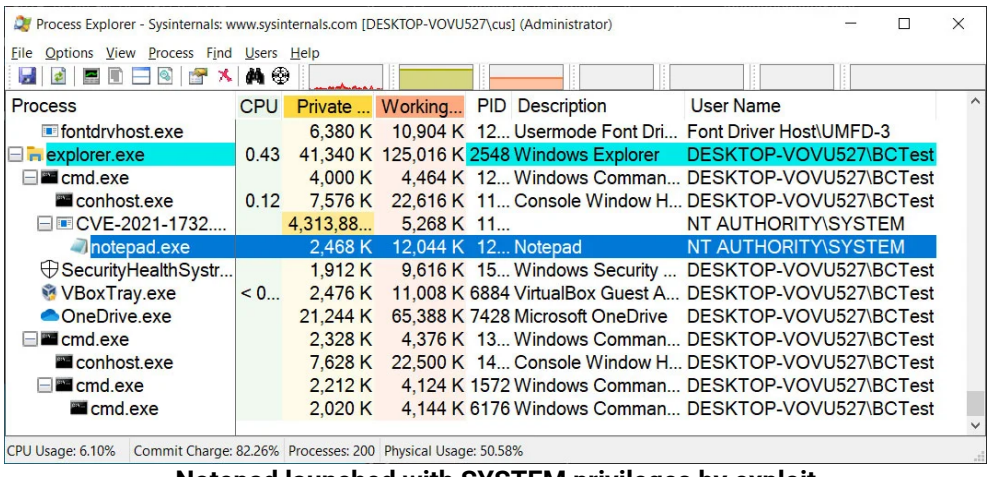
Microsoft attributes the discovery of this vulnerability to RyeLv (https://twitter.com/b2ahex), who shared a technical analysis (http://googleprojectzero.github.io/0days-in-the-wild//0day-

RCAs/2022/CVE-2022-21882.html) of the vulnerability after Microsoft released the patch.

This week, multiple exploits were publicly released for CVE-2022-21882 that allow anyone to gain SYSTEM privileges on vulnerable Windows 10 devices.

After the exploit's release, Will Dormann, a vulnerability analyst for CERT/CC and Twitter's resident exploit tester, confirmed that the exploits works (https://twitter.com/wdormann/status/1487205136174878721) and provides elevated privileges.

BleepingComputer also tested the vulnerability and had no problem compiling the exploit and using it to open Notepad with SYSTEM privileges on Windows 10, as shown below. BleepingComputer could not get the exploit to work on Windows 11.



Notepad launched with SYSTEM privileges by exploit

Source: BleepingComputer

While we only opened Notepad using this exploit, threat actors can also use it to add new users with Administrator privileges or execute other privileged commands.

While we would not normally report on a patched vulnerability, many administrators chose to skip January 2022 updates due to the significant number of critical bugs introduced by the January 2022 updates

(https://www.bleepingcomputer.com/news/microsoft/new-windows-server-updates-cause-dc-boot-loops-break-hyper-v/), including reboots, L2TP VPN problems, inaccessible ReFS volumes, and Hyper-V issues the installation of these updates.

This means that their devices remain unprotected and vulnerable to an exploit that has historically been used in cyberattacks by APT hacking groups.

With the release of these exploits and as Microsoft released OOB updates (https://www.bleepingcomputer.com/news/microsoft/microsoft-releases-emergency-fixes-for-windows-server-vpn-bugs/) that resolve the issues introduced in the January 2022 updates, it is now strongly advised that admins install the updates rather than wait until the February 8th Patch Tuesday.

Bug found two years earlier

This same vulnerability was discovered two years ago (https://twitter.com/_arkon/status/1486449470741135362) by Israeli security researcher and Piiano CEO Gil Dabah (https://twitter.com/_arkon), who decided not to disclose the bug due to the reduced bug bounty rewards (http://twitter.com/_arkon/status/1487005745023537157?ref_src=twsrc%5Etfw) by Microsoft.

Dabah is not alone in his frustrations over Microsoft's diminishing bug bounty rewards.

In November, security researcher Abdelhamid Nacer released a zero-day privilege elevation exploit (https://www.bleepingcomputer.com/news/microsoft/new-windows-zero-day-with-public-exploit-lets-you-become-an-admin/) due to Microsoft's decreasing payouts in their bug bounty program.

"Microsoft bounties has been trashed since April 2020, I really wouldn't do that if MSFT didn't take the decision to downgrade those bounties," Naceri told BleepingComputer at the time.

RyeLv noted in his technical writeup for the CVE-2022-21882 vulnerability that the best way to eliminate this bug class is to improve Microsoft's Windows kernel bug bounties.

"Improve the kernel 0day bounty, let more security researchers participate in the bounty program, and help the system to be more perfect," advised RyeLv.

Related Articles:

Microsoft December 2021 Patch Tuesday fixes 6 zero-days, 67 flaws (https://www.bleepingcomputer.com/news/microsoft/microsoft-december-2021-patch-tuesday-fixes-6-zero-days-67-flaws/)

Attackers can get root by crashing Ubuntu's AccountsService (https://www.bleepingcomputer.com/news/security/attackers-can-get-root-by-crashing-ubuntu-s-accountsservice/)

Microsoft lists the Windows 10 group policies to avoid (https://www.bleepingcomputer.com/news/microsoft/microsoft-lists-the-windows-10-group-policies-to-avoid/)

New Windows KB5009543, KB5009566 updates break L2TP VPN connections (https://www.bleepingcomputer.com/news/microsoft/new-windows-kb5009543-kb5009566-updates-break-l2tp-vpn-connections/)

800K WordPress sites still impacted by critical SEO plugin flaw (https://www.bleepingcomputer.com/news/security/800k-wordpress-sites-still-impacted-by-critical-seo-plugin-flaw/)

ELEVATION OF PRIVILEGES (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/ELEVATION-OF-PRIVILEGES/)

EXPLOIT (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/EXPLOIT/)

MICROSOFT (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/MICROSOFT/)

PRIVILEGE ESCALATION (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/PRIVILEGE-ESCALATION/)

VULNERABILITY (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/VULNERABILITY/)

WINDOWS 10 (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/WINDOWS-10/)

WINDOWS 11 (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/WINDOWS-11/)