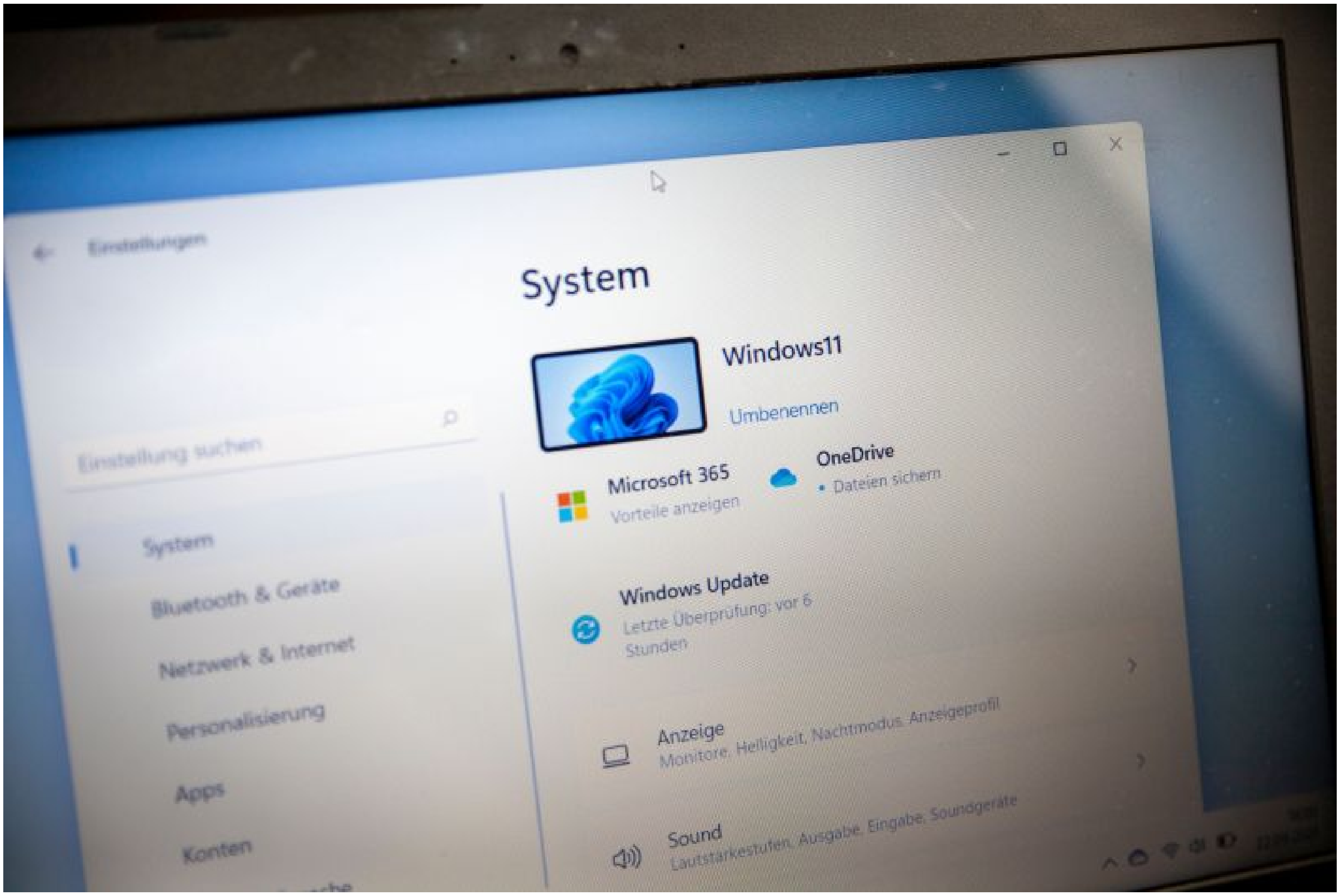
Previous article

Next article

Attackers Actively Target Windows Installer Zero-Day



Author:

Elizabeth Montalbano

November 24, 2021 / 9:09 am

Share this article:

Researcher discovered a “more powerful” variant of an elevation-of-privilege flaw for which Microsoft released a botched patch earlier this month.

Attackers are actively exploiting a Windows Installer zero-day vulnerability that was discovered when a patch Microsoft issued for another security hole inadequately fixed the original and unrelated problem.

Over the weekend, security researcher Abdelhamid Naceri discovered a Windows Installer elevation-of-privilege vulnerability tracked as CVE-2021-41379 that Microsoft patched a couple of weeks ago as part of its November Patch Tuesday updates.

However, after examining the fix, Naceri found a bypass as well as an even more concerning zero-day privilege-elevation bug. The researcher posted a proof of concept (POC) exploit Tuesday on GitHub for the newly discovered bug that he said works on all currently-supported versions of Windows.

If exploited, the POC, called InstallerFileTakeOver, gives an actor administration privileges in Windows 10, Windows 11 and Windows Server when logged onto a Windows machine with Edge installed.

Peer Research Confirms Exploit and Active Attacks

Researchers at Cisco Talos Security Intelligence and Research Group as well as others confirmed the POC can be reproduced as well as corroborating evidence that threat actors were already exploiting the bug.

“This vulnerability affects every version of Microsoft Windows, including fully patched Windows 11 and Server 2022,” according to a post on the Cisco Talos blog by

Jaeson Schultz, technical leader for Cisco Talos. “Talos has already detected malware samples in the wild that are attempting to take advantage of this vulnerability.”

Other researchers also confirmed on Twitter that the POC functions as advertised to deliver local privilege escalation.

“Can confirm this works, local priv esc,” tweeted security researcher Kevin Beaumont, who said he tested it on Windows 10 20H2 and Windows 11. “The prior patch MS issued didn’t fix the issue properly.”

Discovery and More Details

As detailed by Microsoft, CVE-2021-41379 is a Windows Installer elevation of privilege vulnerability with a rating of low on the Common Vulnerability Scoring System.

"An attacker would only be able to delete targeted files on a system," according to Microsoft's notes on the flaw. "They would not gain privileges to view or modify file contents."

However, Microsoft's patch for the bug did not fix the vulnerability correctly, allowing Naceri to bypass it during his analysis of the patch, he said in his GitHub post of the POC.

However, that bypass was small potatoes compared to a variant of CVE-2021-41379 that he discovered during his research that is "more powerful than the original one," which is why Naceri chose to publish a POC of that flaw instead, he wrote.

The code Naceri released leverages the discretionary access control list (DACL) for Microsoft Edge Elevation Service to replace any executable file on the system with an MSI file, allowing an attacker to run code as an administrator, Cisco Talos' Schultz explained in his post.

Wait for the Patch

The associated POC works in every supporting windows installation, including Windows 11 and Server 2022 with the November 2021 patch, as well as in server installations, Naceri wrote.

"While group policy by default doesn't allow standard users to do any MSI operation, the administrative install feature thing seems to be completely bypassing group policy," he wrote.

Due to the "complexity" of the vulnerability, Naceri said that the best workaround available for the flaw at this time "is to wait Microsoft to release a security patch.

"Any attempt to patch the binary directly will break Windows installer," he wrote, adding that those affected should "wait and see how Microsoft will screw the patch again" before taking any mitigation action.

A Microsoft spokesperson told BleepingComputer that the company is aware of Naceri's disclosure and "will do what is necessary" to keep customers "safe and protected," according to a published report.

"An attacker using the methods described must already have access and the ability to run code on a target victim's machine," the spokesperson said, according to the report.

find out how this open-source tool can help tame security across your organization's entire campus.

Register NOW to access the on-demand event!

Write a comment

Share this article:

Malware Vulnerabilities

SUGGESTED ARTICLES

New Twists on Gift-Card Scams Flourish on Black Friday

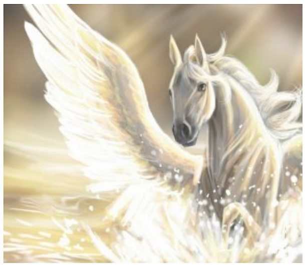
Fake merchandise and crypto jacking are among the new ways cybercriminals will try to defraud people flocking online for Black Friday and Cyber Monday.

November 25, 2021

9.3M+ Androids Running 'Malicious' Games from Huawei AppGallery

A new trojan called Android.Cynos.7.origin, designed to collect Android users' device data and phone numbers, was found in 190 games installed on over 9M Android devices.

November 24, 2021



Apple's NSO Grou Amps Up Pressure Spyware-Maker

Just weeks after a judge Group did not have imr brought by Facebook su WhatsApp, Apple is add weight to the company

November 24, 2021

DISCUSSION

Leave A Comment

Write a reply...

Your name

Your email

Send Comment

This site uses Akismet to reduce spam. Learn how your comment data is processed.

INFOSEC INSIDER

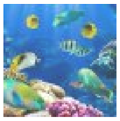
How to Defend Against Mobile App Impersonation

November 23, 2021

Online Merchants: Prevent Fraudsters from Becoming Holiday Grinches

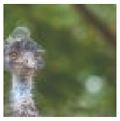
November 22, 2021

3 Top Tools for Defending Against Phishing Attacks



November 18, 2021

Rooting Malware Is Back for Mobile. Here’s What to Look Out For.



November 16, 2021

Top 10 Cybersecurity Best Practices to Combat Ransomware

November 12, 2021 6

Twitter

Pankaj Gupta, Senior Director at @Citrix, outlines how distributed denial of service attacks have become increasing… https://t.co/djwhuUE82e

1 week ago

Follow @threatpost

The First Stop For Security News

Privacy Policy

Terms and Conditions

Advertise