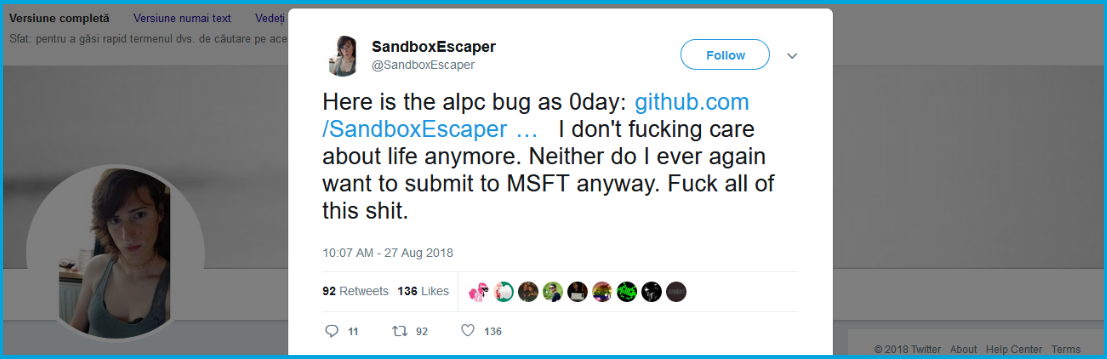
kindred

Security Newsletter

3 September 2018

Subscribe to this newsletter

Exploit Published for Unpatched Flaw in Windows Task Scheduler



SandboxEscaper
@SandboxEscaper

Here is the alpc bug as 0day: github.com/SandboxEscaper … I don't fucking care about life anymore. Neither do I ever again want to submit to MSFT anyway. Fuck all of this shit.

10:07 AM - 27 Aug 2018

92 Retweets 136 Likes

Versiune completă
Versiune numai text
Vedeți
Sfat: pentru a găsi rapid termenul dvs. de căutare pe ace
Follow
11
92
136
© 2018 Twitter About Help Center Terms

A security researcher has published on Twitter details about a vulnerability in the Windows OS. The vulnerability is a "local privilege escalation" issue that allows an attacker to elevate the access of malicious code from a limited USER role to an all-access SYSTEM account.

Will Dormann, an engineer of CERT/CC, has confirmed the vulnerability and has issued an official CERT/CC alert last night. Dormann says the vulnerability resides in the Windows Task Scheduler, and more precisely in the Advanced Local Procedure Call (ALPC) interface.

The researcher, who goes online by the name of SandboxEscaper, has released proof-of-concept (PoC) code on GitHub for exploiting the ALPC interface to gain SYSTEM access on a Windows system. Malware authors will particularly be interested in this PoC, as it allows benign malware to gain admin access on targeted systems using an exploit more reliable than many existing methods. SandboxEscaper has not notified Microsoft about the vulnerability, meaning there is no official patch for this flaw. Currently, all Windows 64-bit users are vulnerable. The zero-day flaw has been confirmed working on a "fully-patched 64-bit Windows 10 system."

A patch is available for the Windows zero-day, but it’s not from Microsoft. Instead, the fix comes from 0patch, a community project that aims at addressing software vulnerabilities by delivering tiny fixes to users worldwide. The fix for this week’s vulnerability is also very small, at only 13 bytes. It was released within 24 hours after the bug was ousted on Twitter on Monday, and, already validated and verified, it is now rolling out to users.

Read More

Even More

Third-Party Patch Released for Windows Zero-Day

Critical Flaw Fixed in Packagist, PHP's Largest Package Repository

The maintainers of Packagist, the PHP ecosystem's largest package repository, have fixed a critical vulnerability on their official website that could have allowed an attacker to hijack their service. The flaw was discovered and reported by security researcher Max Justicz.

According to Justicz, the "Submit Package" input field for submitting new PHP packages via the Packagist homepage allowed an attacker to run a malicious command in the format of "$(MALICIOUS_COMMANDS)". Justicz discovered that Packagist was improperly escaping inputted characters when performing checks to see if the URL leads to a Perforce or Subversion repository, and was executing the malicious commands.

Packagist is not a package manager, but only a host for PHP packages. It is the default package host behind Composer, the most popular PHP package manager. Packagist is the largest package hosting service in the PHP ecosystem, with over 435 million package installs reported in July 2018 alone.

Read More

Even More

Cutting room floor

- WireGuard VPN review: A new type of VPN offers serious advantages
- Air Canada resets 1.7 million accounts after app breach
- Firefox: Changing Our Approach to Anti-tracking
- Pwned Passwords, Now As NTLM Hashes!
- One in five employees share their email password with co-workers
- Fiserv Flaw Exposed Customer Data at Hundreds of Banks
- Conceptual and Technical Challenges in Multi-cloud Security
- Data of 130 Million Chinese Hotel Chain Guests Sold on Dark Web Forum
- No, eight characters, some capital letters and numbers is not a good password policy
- Fortnite CEO mad at Google for revealing security hole early
- Building the security operations center of tomorrow—harnessing the law of data gravity
- Google 'Titan Security Key' Is Now On Sale For $50

#Tech and #Tools

- Remote Code Execution on packagist.org
- How We Micropatched a Publicly Dropped 0day in Task Scheduler (CVE-UNKNOWN)
- Remote Code Execution on a Facebook server
- LAteral Movement Encryption technique (a.k.a. The "LAME" technique)
- Firework: Leveraging Microsoft Workspaces in a Penetration Test
- Native Android Proxmark3 client (no root required)
- Playing with the new Burp suite REST API
- Bypassing Workflows Protection Mechanisms - Remote Code Execution on SharePoint
- Assume the Worst: Enumerating AWS Roles through 'AssumeRole
- Three C-Words of Web App Security: Part 1 – CORS
- From Compiler Optimization to Code Execution - VirtualBox VM Escape - CVE-2018-2844
- Apache Struts2 CVE-2018-11776 POC
- nmap-parse-output: A tool for analyzing Nmap scans

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with over 15 million customers across 100 markets. We offer pre-game and live Sports betting, Poker, Casino and Games through 13 subsidiaries and brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and as an innovation driven company that builds on trust.

You can access the previous newsletters at https://news.infosecgur.us