UAC BYPASS WITH ELEVATED PRIVILEGES WORKS ON ALL WINDOWS VERSIONS

Security Newspaper | August 19, 2016 | Important, Incidents, Malware, Vulnerabilities | No Comments

Microsoft delays fixing the reported issue. enSilo senior security researcher Yotam Gottesman has discovered a simple method of bypassing the Windows User Account Control (UAC) mechanism that affects all supported Windows versions, which in some exploitation scenarios leads to attackers executing commands with elevated privileges.

The technique Gottesman discovered relies on the methods used to interact and control environment variables.

Windows environment variables are a set of temporary settings that are specific to each Windows process and are inherited by their child processes, which can read and write their values.

Windows-level environment variables and their capabilities

Unknown to the vast majority of users is that there are a class of system-wide environment variables that apply to the entire Windows operating system.

These include details like the user's current username, the PC's domain, and file paths for various folders such as the Windows OS, AppData, user profile, and so on.

This set of environment variables are stored in the Windows Registry, hence they are automatically persistent across reboots and can also be modified by any user via "set" or "setx" commands.

UAC bypasses get worse when combined high-privileged applications

But there is more. Because of the way Windows is built, there are special apps that, when launched by regular users, execute processes with higher privileges (Task Manager, Disk Cleanup – known UAC bypass, Event Viewer – known UAC bypass, more).

When a user launches one of these apps, Windows UAC trusts its execution by default and does not show a warning.

Crooks can use modified environment variables to spawn malicious child processes under the legitimate app and execute an attack. Windows UAC will stay quiet while the attack runs with elevated privileges because UAC trusts the parent process.

Proof-of-concept attacks that work

Gottesman described five types of attacks, which can be combined, in a technical write-up for enSilo.

In one example, an attacker can create a copy of the C:/Windows folder and modify the system-wide environment variable to point to the wrong Windows OS folder. This setting activates after a system reboot and allows the attacker to load malicious DLLs on the system.

This doesn't mean the attacker has hijacked the OS, but when other legitimate apps need to load a system DLL, they'll be pointed to the wrong location, where the attacker can easily modify and replace files without security products warning the user.

In another similar attack, he tricked Windows into loading the same C:/Windows folder from a local network folder, meaning the malicious DLLs don't even have to be stored on the same filesystem.

Triggering a malicious child process with elevated privileges via legitimate app and hijacked Windows environment variables

ℹ *Triggering a malicious child process with elevated privileges via legitimate app and hijacked Windows environment variables*

In his examples, Gottesman was able to load mmc.exe, the Windows management console with elevated privileges under svchost.exe, meanwhile loading a malicious DLL from the attacker's


Apache Struts Jakarta Multipart Parser Remote Code…


HIJACKING WHATSAPP ACCOUNTS USING WHATSAPP WEB


Extracting Hashes & Plaintext Passwords from Windows 10


Best Hacking Tools Of 2017 For Windows, Linux, And OS X


10 Best Password Cracking Tools Of 2016 | Windows,…


UBER HACKING: HOW WE FOUND OUT WHO YOU ARE, WHERE…


DoublePulsar Initial SMB Backdoor Ring 0 Shellcode Analysis


Hack Remote Windows PC using The Backdoor factory…


US Army Experts Call for military bug bounty program AVRP

Hacking Facebook Accounts with just a phone number…

C:/copied/Windows folder. This was done with no UAC warning and with elevated privileges.

A Windows patch will be coming in the future

The enSilo researcher notified Microsoft, but the company classified this as a UAC bypass issue, and not an elevation of privileges flaw. Microsoft doesn't consider UAC bypass a security flaw, meaning it won't get patched with the utmost urgency but will eventually be dealt with in the future. Proof-of-concept code is available on GitHub.

"Environment variable expansion in Windows allows an attacker to gather information about a system prior to an attack and eventually take complete and persistent control of the system at the time of choice by running a single user-level command, or alternatively, changing one registry key," Gottesman explains.

"This vector also lets the attacker's code in the form of a DLL to load into legitimate processes of other vendors or the OS itself and masquerade its actions as the target process' actions without having to use code injection techniques or use memory manipulations," the researcher also added. "3rd party services that run on behalf of an administrator may also be vulnerable to this attack and allow regular users to elevate their privileges inside the system."

Researcher running his exploit demo

Researcher running his exploit demo
Source:http://news.softpedia.com/
(Visited 257 times, 1 visits today)

Tags: malicious DLLs, UAC Bypass

RELATED POSTS

RECENT NEWS

- Internet Explorer zero-day: browser is once again under attack
- SynAck targeted ransomware uses the Doppelgänging technique
- How to do reconnaissance attack over your target the correct way
- Throwhammer the New Way to Launch Rowhammer Attacks via Network Packets
- IBM improves its security and prohibits the use of USB drives throughout the company
- You must update 7-zip now! critical vulnerability found
- Vulnerabilities in LG smartphones exploited to execute remote code
- Researchers Found Backdoor in Python Library That Steal SSH Credentials
- BaseStriker the new attack for Microsoft Office 365
- Hackers attack Copenhagen city's bicycle sharing system

CATEGORIES

- Data Security

FBI HACKS INTO TERRORIST'S IPHONE WITHOUT APPLE

No Comments | Mar 29, 2016

VULNERABILITY IN SKYPE ALLOWS YOU TO OBTAIN PRIVILEGES AT THE SYSTEM LEVEL

No Comments | Feb 15, 2018

HOW TO PROTECT YOURSELF FROM WANNACRY RANSOMWARE?

No Comments | May 15, 2017

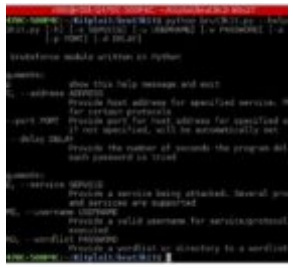
ZERO-DAY, ANGLER KIT EXPLOITS HELP DRIVE UP MALVERTISING BY 325%

No Comments | Aug 28, 2015

- Important
- Incidents
- Malware
- Mobile Security
- Technology
- Vulnerabilities

IMPORTANT

HOW TO DO RECONNAISSANCE ATTACK OVER YOUR TARGET THE CORRECT WAY



TOOL TO PERFORM BRUTE FORCE ATTACKS ON SSH, SMTP, FACEBOOK AND INSTAGRAM- BRUT3K1T

HOW TO HACK ANY CAR WITH THIS TOOL

HOW TO DO OFFENSIVE PENETRATION TESTING WITH KALI?

HACK ANY WIRELESS NETWORK USING ALL IN ONE TOOL: HIJACKER

TRUSTJACKING ATTACK ALLOWS HACKERS TO HACK IOS DEVICES