ZERO DAY INITIATIVE

SUBSCRIBE

THANKSGIVING TREAT: EASY-AS-PIE WINDOWS 7 SECURE DESKTOP ESCALATION OF PRIVILEGE

November 19, 2019 | Simon Zuckerbraun

It is to escalate to SYSTEM.

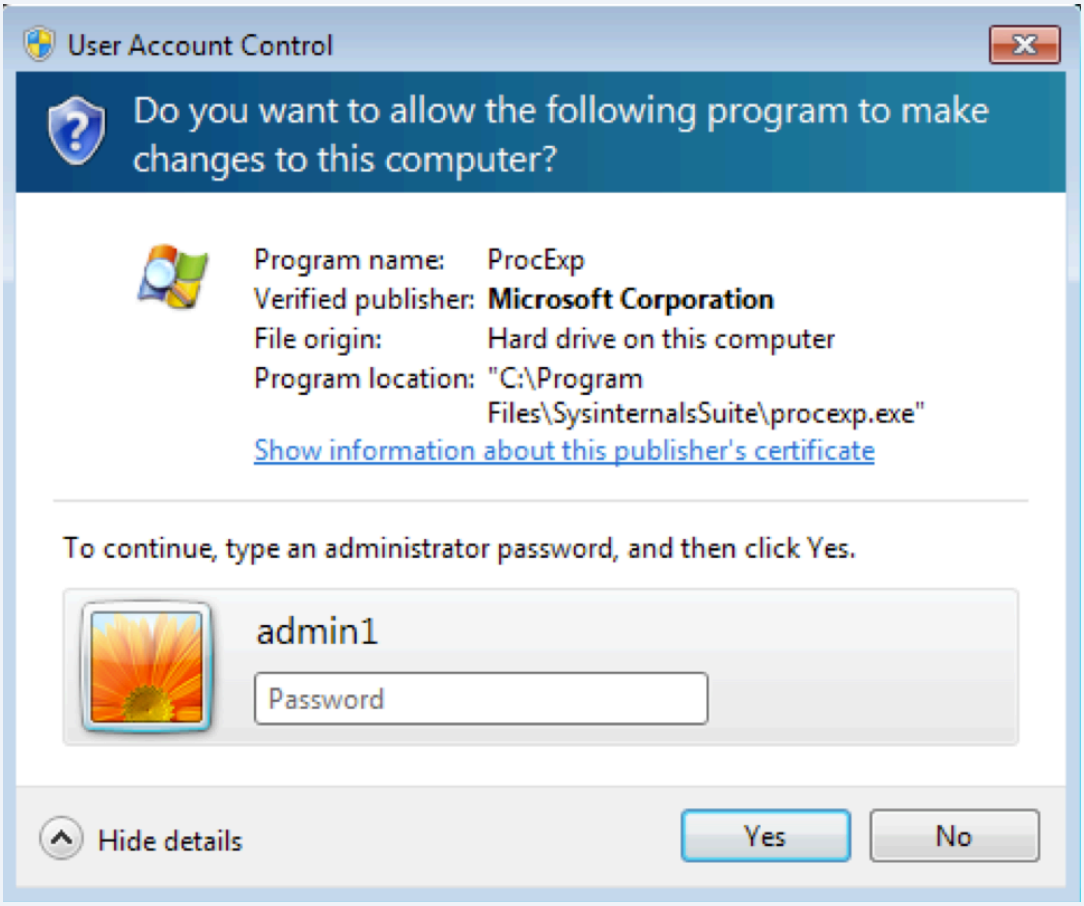
The bug is found in the UAC (User Account Control) mechanism. By default, Windows shows all UAC prompts on a separate desktop known as the Secure Desktop. The prompts themselves are produced by an executable named `consent.exe`, running as `NT AUTHORITY\SYSTEM` and having an integrity level of System. Since the user can interact with this UI, it is necessary for the UI to be very tightly constrained. Otherwise, a low privileged user might be able to perform actions as SYSTEM via a circuitous route of UI operations. Even a solitary UI feature that appears harmless in isolation could potentially be the first step in a chain of actions leading to arbitrary control. Indeed, you will find that the UAC dialogs are stripped down to contain a bare minimum of clickable options.

Shall we go exploring a bit?

We can enter the UAC prompts by right-clicking any executable and choosing Run as administrator... That will bring up a dialog on the Secure Desktop that looks like this:

Not much interesting so far, just Yes and No buttons, a password input field, and an X button. You can click the upper-left corner of the window and get the standard, little-used "window menu", having just Move and Close commands. The password input field is a bit interesting to poke around in. Perhaps it could give you some way to open up additional UI features, via an IME, for example. I have tried, though, and not uncovered anything.

All right, but what of that "Show details" option?



This is a promising route, since, as you probably know, the Windows certificate dialog allows you to export a displayed certificate to a file. That would give us access to the standard File Save dialog, opening up a wealth of UI functionality. Will it work?

Drat, Microsoft has grayed out the button! And to think, we almost got away with it. I seem to recall having tried that one years ago.

But here's what you probably don't know about the certificate dialog: There is an obscure Microsoft-specific object identifier (OID) defined, having the numeric value `1.3.6.1.4.1.311.2.1.10`. The `WinTrust.h` header defines this as `SPC_SP_AGENCY_INFO_OBJID`,

It appears, however, that the certificate dialog parses the value of this OID, and if it finds valid and properly-formatted data, it will use it to render the "Issued by" field on the General tab as a hyperlink! And when it comes to the UAC version of the certificate dialog, Microsoft forgot to disable this hyperlink.

The finder of this bug provided us with a copy of an ancient Microsoft-signed executable that has such a certificate:

Clicking on the hyperlink will launch a browser from consent.exe, and the browser will run as `NT AUTHORITY\SYSTEM`. Quite strangely, even though the browser is launched as SYSTEM, nevertheless it is shown on the normal desktop as opposed to the Secure Desktop. Hence it will only become visible once the user has exited all the UAC dialogs. From the attacker's perspective, this is an ideal combination.

In action, this vulnerability is a wonder to behold. In my mind at least, it's an instant classic. The video below shows the complete process,

Microsoft patched this vulnerability in November 2019 as CVE-2019-1388. In their writeup, they state the fix was implemented by "ensuring Windows Certificate Dialog properly enforces user privileges." However, they also give an Exploit Index rating of 2, indicating exploitation is less likely. Our video suggests otherwise.

Here at the Zero Day Initiative we're thankful for all the great bugs our talented submitters have sent us in this past year, and we wish everyone a prosperous 2020.

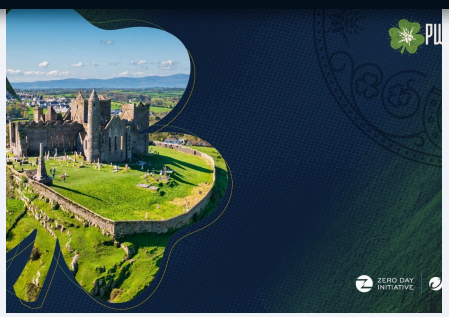
You can find me on Twitter at @HexKitchen, and follow the team for the latest in exploit techniques and security patches.

Microsoft Windows Research UAC

ZERO DAY INITIATIVE

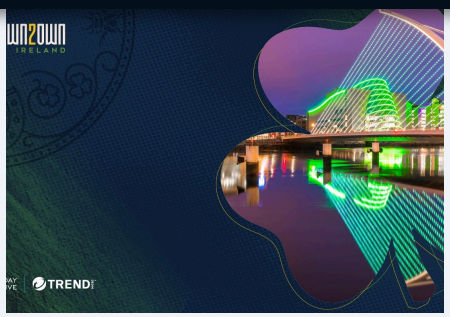
PWN2OWN IRELAND 2024: DAY FOUR AND MASTER OF PWN

Pwn2Own



PWN2OWN IRELAND 2024: DAY THREE RESULTS

Pwn2Own



PWN2OWN IRELAND 2024: DAY TWO RESULTS

Pwn2Own, Samsung, Canon

General Inquiries
zdi@trendmicro.com

Find us on X
@thezdi

Find us on Mastodon
Mastodon

Media Inquiries
media_relations@trendmicro.com

Sensitive Email Communications
PGP Key