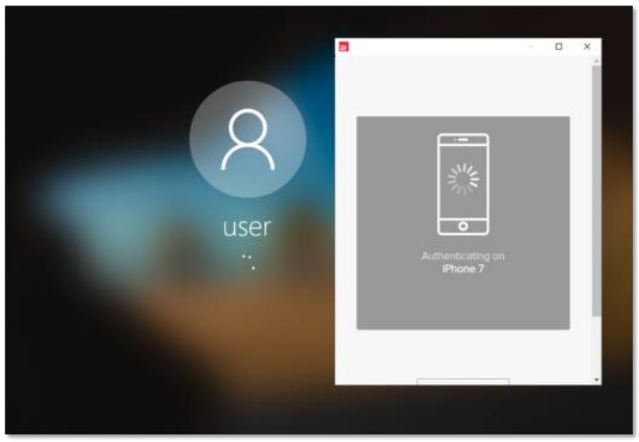
Authored 2 years ago by Julian Scionti

# CVE-2020-25826 - PingID Integration for Windows Login Local Privilege Escalation

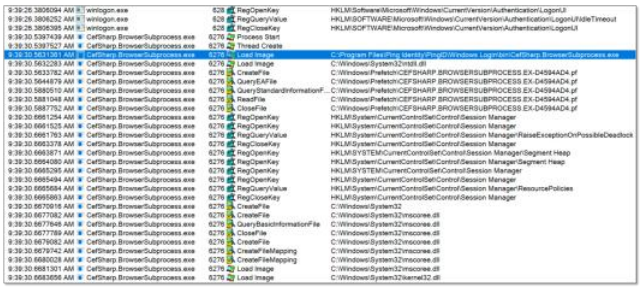
PingID offers a Windows Login desktop agent which adds 2FA to the Windows Logon process.

Here it is in action:

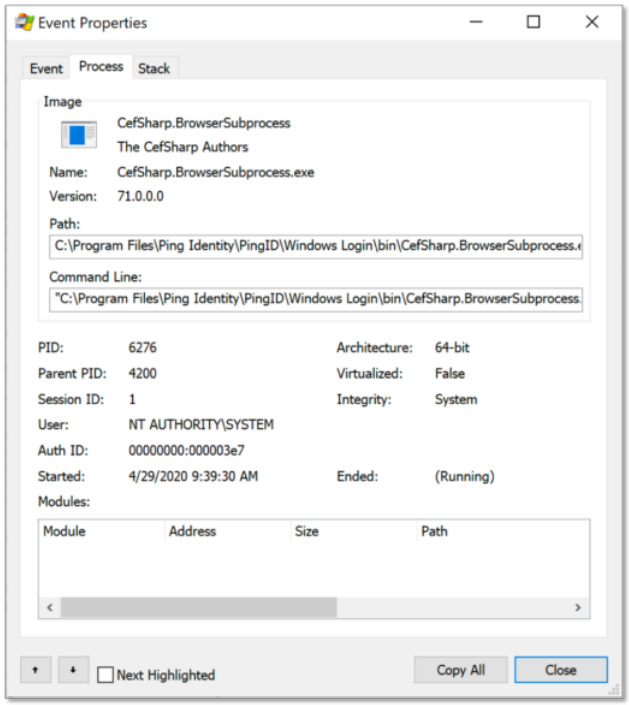



The `winlogon.exe` process runs as `NT AUTHORITY\SYSTEM`, so processes started before you login to Windows also run as `SYSTEM`. This feature of Windows has a history of being abused by APTs[1] by backdooring Windows Accessibility Features (like sticky keys or the on-screen keyboard). So when PingID prompts a user for 2FA, their agent is going to be executed with `SYSTEM` privileges.

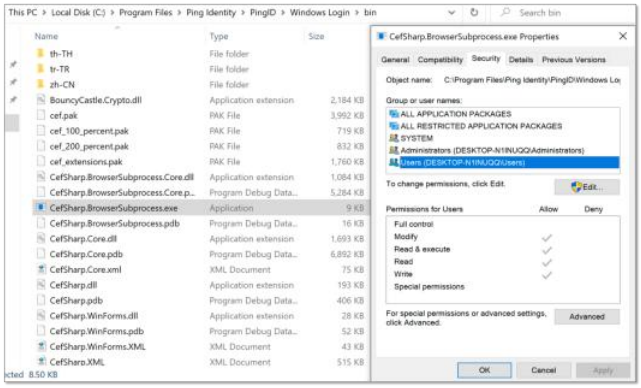
Here's a screencap from procmon after relogging to look at execution flow...



... and here's a screenshot showing that the agent is running with `SYSTEM` privielges.




So what's the problem? Well, the way that the agent is installed allows for unprivileged users to modify *everything*.




By overwriting the `CefSharp.BrowserSubprocess.exe` with `cmd.exe`, for example, a malicious user could get a command prompt shell running as SYSTEM by locking the machine and entering a valid password. Another, more elegant solution, is to create a DLL crafted with malicious code which an attacker could place into the "C:\Program Files\Ping Identity\Windows Login\Bin" directory, overwriting a DLL used by the agent.

This issue was patched in version 2.4.2[2].

Edited 2 years ago

**References** 123 bytes

```
1. https://attack.mitre.org/techniques/T1546/008/
2. https://docs.pingidentity.com/bundle/pingid/page/xqr1597139945488.html
```