1030 - WSUSpendu: How to hang WSUS clients

Saturday at 10:30 in Track 3
h
20 minutes | Demo, Tool

Romain Coltel*Lead product manager at Alsid*

Yves Le Provost*Security auditor at ANSSI*

You are performing a pentest. You just owned the first domain controller. That was easy. All the computers are belong to you. But unfortunately, you can't reach the final goal. The last target is further in the network, non accessible and heavily filtered. Thankfully, one last hope remains. You realize the target domain pulls its updates from the WSUS server of the compromised domain, the one you fully control. Hope is back... But once again, it fails. The only tools available for controlling the updates are not working: they require a network attack that is prevented by the network architecture and the server configuration. All hope is lost...

We will present you a new approach, allowing you to circumvent these limitations and to exploit this situation in order to deliver updates. Thus, you will be able to control the targeted network from the very WSUS server you own. By extension, this approach may serve as a basis for an air gap attack for disconnected networks.

Our talk will describe vulnerable architectures to this approach and also make some in-context demonstration of the attack with new public tooling. Finally, as nothing is inescapable, we will also explain how you can protect your update architecture.

Romain Coltel

Romain Coltel is the lead product manager in a french startup, Alsid IT, tackling Active Directory problems down to the core, and he's thus currently doing a lot of research and development on various Active Directory technologies. He's also teaching the well-received SANS SEC660 in France, each time with the author's congratulations at the end of the session.

Before that, he was acquiring his experience in the french National Cybersecurity Agency (ANSSI) as an IT auditor, where he performed penetration testing, various security researches and tools development. As a development example, he's the lead developer of dislocker, a tool to decrypt BitLocker-encrypted partitions on Linux, OSX and FreeBSD. He also implemented the AES-XEX and -XTS modes for the famous mbedTLS library.

Yves Le Provost

Yves Le Provost is a security auditor for more than 10 years. He's working for ANSSI, the french National Cybersecurity Agency since 5 years ago. During these five years defending french administrations, he specialized in database security, OS internals, SCADA architecture and penetration testing.

In parallel, he's teaching french engineering schools about various security topics.

#defcon25/by_track/track3/saturday #defcon25/By_Day/_saturday