ZEROLOGON: INSTANTLY BECOME DOMAIN ADMIN BY SUBVERTING NETLOGON CRYPTOGRAPHY (CVE-2020-1472)

Blog post 11 September 2020 by Tom Tervoort, Senior Security Specialist and Ralph Moonen, Technical Director at Secura

Last month, Microsoft patched a very interesting vulnerability 'zerologon' that would allow an attacker with a foothold on your internal network to essentially become Domain Admin with one click. All that is required is for a connection to the Domain Controller to be possible from the attacker's viewpoint.

Secura's security expert Tom Tervoort previously discovered **a less severe Netlogon vulnerability last year that allowed workstations to be taken over**, but the attacker required a Person-in-the-Middle (PitM) position for that to work. Now, he discovered this second, much more severe (CVSS score: 10.0) vulnerability in the protocol. By forging an authentication token for specific Netlogon functionality, he was able to call a function to set the computer password of the Domain Controller to a known value. After that, the attacker can use this new password to take control over the domain controller and steal credentials of a domain admin.

The vulnerability stems from a flaw in a cryptographic authentication scheme used by the Netlogon Remote Protocol, which among other things can be used to update computer passwords. This flaw allows attackers to impersonate any

Secura urges everybody to install the patch on all their domain controllers as fast as possible. Please refer to Microsoft's advisory. **We published a test tool on Github**, which you can download here: **https://github.com/SecuraBV/CVE-2020-1472** that can tell you whether a domain controller is vulnerable or not.

If you are interested in the technical details behind this pretty unique vulnerability and how it was discovered, **download the whitepaper below. For more information about the CVE, contact Secura at info@secura.com.**

WHITEPAPER

Would you like to learn more about Secura's Vulnerability Assessments? Please fill out the form and we will contact you within one business day.

TOM TERVOORT

Principal Security

RALPH MOONEN

Technical Director

Phone Number

Email Address *

Message *

□ I give permission to process my data as described in the Privacy Policy.

SUBMIT

RELATED SERVICES

OVER SECURA

Secura is een toonaangevend bedrijf op het gebied van cyberbeveiliging. Onze klanten variëren van overheid en zorg tot financiën en industrie. Secura biedt technische diensten aan, zoals vulnerability assessments, penetratietesten en Red Teaming. We bieden ook certificering voor IoT en industriële omgevingen, evenals audits, forensische diensten en awarenesstrainingen.

Ons doel is om uw cyberweerbaarheid te vergroten. Wij zijn een Bureau Veritas-bedrijf. Bureau Veritas (BV) is een beursgenoteerde onderneming die gespecialiseerd is in testen, inspecteren en certificeren. BV is opgericht in 1828, heeft ruim 80.000 medewerkers en is actief in 140 landen. Secura is de hoeksteen van de cyberbeveiligingsstrategie van Bureau Veritas.

-

At Secura/Bureau Veritas, we are dedicated to being your trusted partner in cybersecurity. We go beyond quick fixes and isolated services. Our integrated approach makes sure that every aspect of your company or organization is cyber resilient, from your technology to your processes and your people.

Secura is the cybersecurity division of Bureau Veritas, specialized in testing, inspection and certification. Bureau Veritas was founded in 1828, has over 80.000 employees and is active in 140 countries.

Cookie Declaration

en
ic

info@secura.com