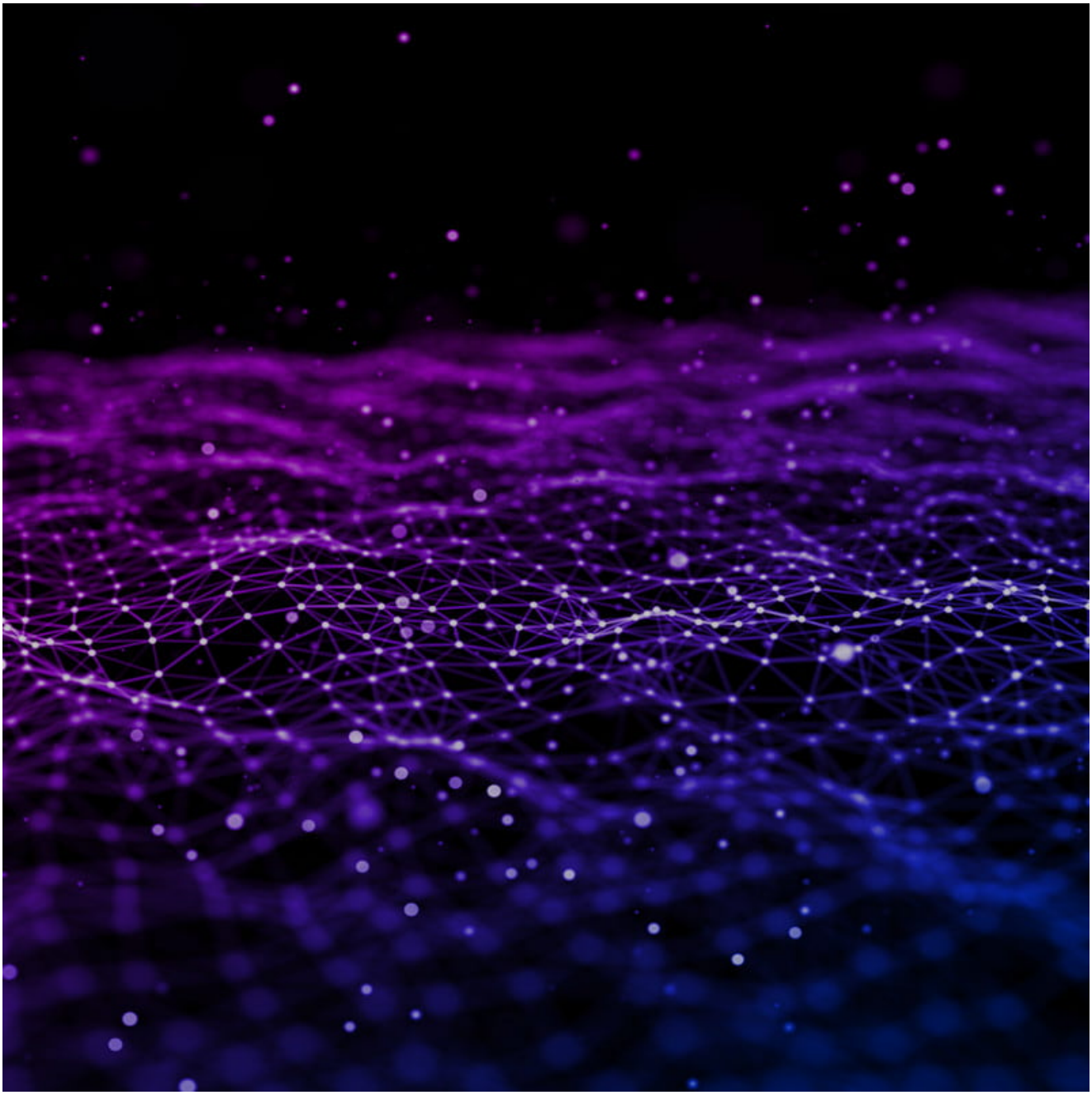
noPac: A Tale of Two Vulnerabilities That Could End in Ransomware

secureworks.com/blog/nopac-a-tale-of-two-vulnerabilities-that-could-end-in-ransomware

Counter Threat Unit Research Team and Incident Response Team



Numerous public proof-of-concept exploits reveal that the noPac vulnerabilities (CVE-2021-42278 and CVE-2021-42287) are trivial to exploit and lead to privilege escalation. Friday, December 17, 2021 *By: Counter Threat Unit Research Team and Incident Response Team*

While the focus in mid-December 2021 has been on Log4j vulnerabilities, two weaponized Windows privilege escalation vulnerabilities (CVE-2021-42278 and CVE-2021-42287) also pose a serious risk to organizations. These vulnerabilities, which are collectively referred to as noPac, enable a threat actor to gain control over a domain controller in matter of minutes.

CVE-2021-42287 is a privilege escalation vulnerability associated with the Kerberos Privilege Attribute Certificate (PAC) in Active Directory Domain Services (AD DS). CVE-2021-42278 is a Security Account Manager (SAM) spoofing security bypass vulnerability. Threat actors could leverage these flaws to escalate to domain administrator privileges from a standard user account.

Gaining domain administrator access

NoPac relies on changing the SamAccountName of a computer account to the name of a domain controller. By default, every authenticated user can add up to ten computers to the domain. The exploitation process includes the following steps:

1. Create a new computer account in Active Directory (AD) with a random name, and then rename it to one of the domain controllers without the trailing $ (see Figure 1).

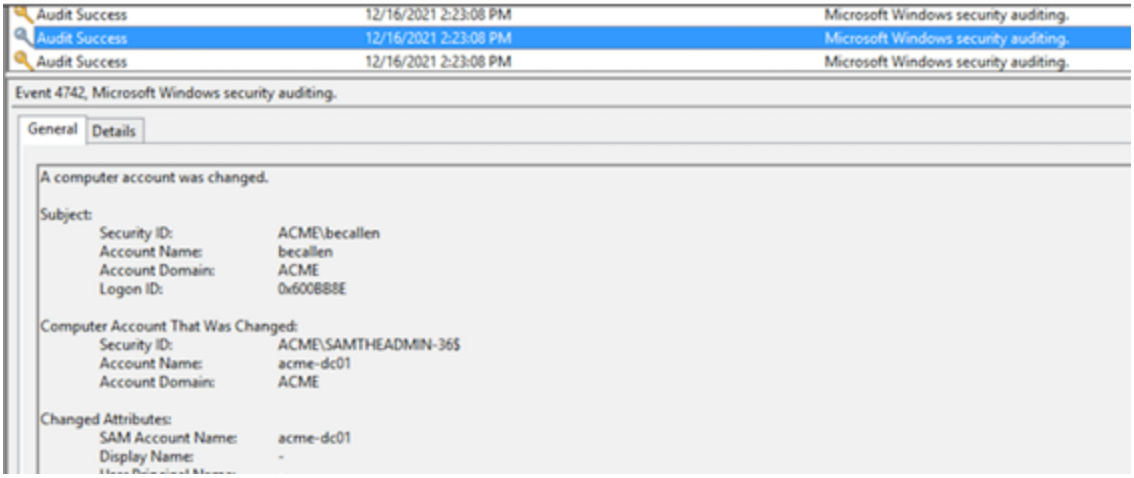


Figure 1. Renaming a user account to spoof a domain controller. (Source: Secureworks)

2. Request a Kerberos ticket-granting ticket (TGT) for the created computer account from step one. Once the ticket is granted, change the name of the computer account back to its original value (see Figure 2).

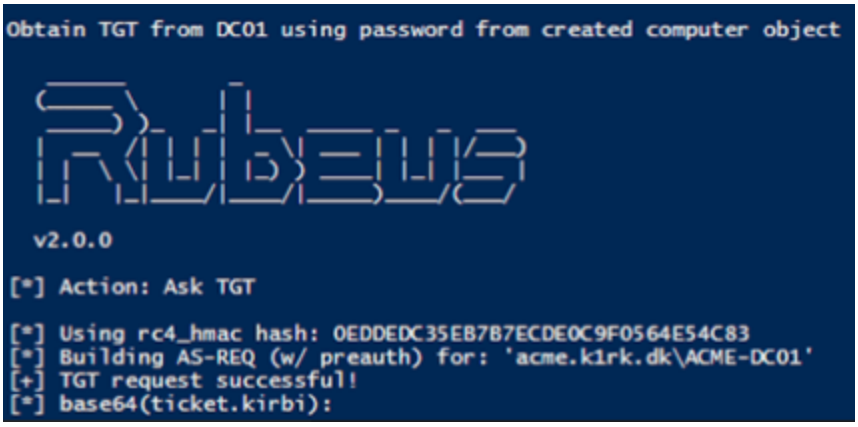


Figure 2. Successful ticket request for spoofed domain controller. (Source: Secureworks)

3. Request a Kerberos ticket granting service (TGS) for the Lightweight Directory Access Protocol (LDAP) service using the TGT from step two with the name of the spoofed domain controller from step one. Because there is no longer an account with that name, TGS chooses the closest match and appends an $. Access to the service is granted, and domain administrator access is acquired (see Figure 3).

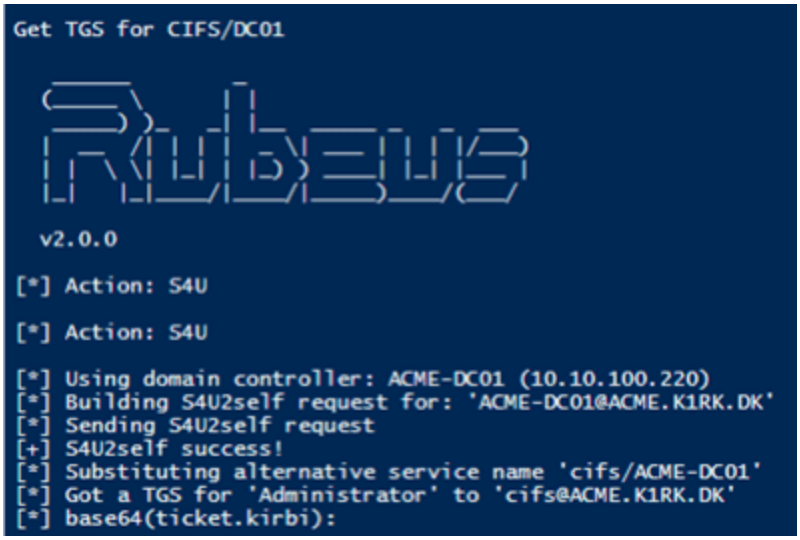


Figure 3. Successful service request for spoofed domain controller. (Source: Secureworks)

Timing is everything

Secureworks® researchers confirmed that exploitation of the noPac vulnerability can be accomplished in as little as 16 seconds. The following video demonstrates real-time domain administrator access.

Potential precursor to ransomware infections

After gaining domain access, a threat actor's ability to deploy additional malware, including ransomware, is virtually unlimited. AD abuse is involved in most ransomware incidents Secureworks researchers investigate. Threat actors typically leverage misconfigurations to escalate privileges within AD. In this case, AD design flaws create the escalation path.

Conclusion

Organizations should immediately apply the applicable Microsoft patches to **all** domain controllers in their environments. These patches include the November 9, 2021 releases for CVE-2021-42278 and CVE-2021-42287, as well as the November 14 out-of-band update. If one domain controller is overlooked, the domain remains vulnerable. Organizations should also follow Microsoft guidance to phase updates for CVE-2021-42287 and restrict users' ability to join workstations to a domain. As of December 17, Secureworks researchers have not observed noPac exploitation in the wild but recommend that organizations remain vigilant.

If you need urgent assistance with an incident, contact the Secureworks Incident Response team. For other questions on how we can help, use our general contact form.