PACRequestorEnforcement and Kerberos Authentication

Joe Dibley

During the November 2021 Patch Tuesday, Microsoft released new security updates for Kerberos. They include new system events and new structures in the Kerberos Privileged Attribute Certificate (PAC). Let's look see what impacts these updates may have on operations and Kerberos ticket-based attacks.

What's new?

As per standard Microsoft updates, there are some new KB articles as well as protocol updates. The one we will be focusing on here is KB5008380, which details the updates for CVE-2021-42287.

Handpicked related content:

[Free Guide] Privileged Access Management Best Practices

PACRequestorEnforcement Registry Key

The updates have both a deployment phase and an enforcement phase. For testing and speed, you can implement enforcement anytime before the enforcement update comes out (currently scheduled for July 12, 2022).

You can configure the behaviour of the patch by applying the DWORD registry key *PACRequestorEnforcement* at *HKEY_LOCAL_MACHINESystemCurrentControlSetServicesKdc* on your domain controllers.

PACRequestorEnforcement can have the following values:

VALUE	BEHAVIOR
0	Disabled — Reverts the update
1 (default)	Deployment — Adds the new PAC. If an authenticating user has the new PAC structure, the authentication is validated.
2	Enforcement — Adds the new PAC. If an authenticating user does not have the new PAC, the authentication is denied.

Protocol Updates

The November 2021 updates also included multiple protocol updates for Kerberos and Active Directory; you can find an overview of them here. For more details, you'll need to look at the errata and then the diff document in the errata.

Updated PAC Structure

The Privileged Attribute Certificate is used to encode authorization information for authenticated users; it contains group memberships, SID history and general user information. In the Nov 2021 updates, Microsoft added two new data structures inside the PAC: PAC_ATTRIBUTES_INFO and PAC_REQUESTOR. When PACRequestorEnforcement is set to 2, both new fields are required for the Kerberos ticket to be successful.

One of the more interesting parts of the updates is the new validation introduced with the PAC_REQUESTOR structure. When this structure is included in a Kerberos ticket, the KDC (domain controller) now validates that the client name (cname) (also referred to as the username) resolves to the same SID that is used in the PAC_REQUESTOR structure, provided that the client and the KDC are in the same domain. If it does not match, then the TGT that was used is automatically revoked and cannot be used. **This happens only when the client and KDC are in the same domain.**

What does this mean for Golden Tickets?

A Golden Ticket is a forged Kerberos ticket that attackers use to gain access to highly privileged resources for long periods of time by manipulating the PAC.

When enforcement mode is active, tools that make Golden Tickets will be required to use the PAC_REQUESTOR field, which is subject to validation by the domain controller. This means that Golden Tickets for non-existent users are no longer possible when they are all in the same domain. However, it is still possible to use non-existent users with Trust Tickets (Golden Tickets made to authenticate over a trust because the validation is completed only when the account is in the same domain as the domain controller).

The new events (which are detailed in the update notes) can provide further indicators for Golden Tickets, such as badly built or not updated exploits. These new events should be gathered into a SIEM if you are using Windows logging for threat detection. The table below details the different events:

Event ID	Name	Description
38	Requestor Mismatch	The new PAC_REQUESTOR structure was used but the client name (username) did not resolve to the SID used in PAC_REQUESTOR.
37	Ticket without Requestor	A service ticket was requested but the new PAC_REQUESTOR structure was not present.
36	Ticket without a PAC	A service ticket was requested but no PAC was present.

Event ID	Name	Description
35	PAC without Attributes	The new PAC_ATTRIBUTE_INFO structure was not present in the PAC

Problems with the Update

Unfortunately, in the initial release of the November 2021 updates, certain Kerberos delegation scenarios were broken, so a new out-of-band patch was released for customers facing this issue. Sander Berkouwer at DirTeam have a nice write-up on this here, with links to each of the KBs available.

Conclusion

Whilst this is a good update and a step in the right direction, it would be great if we continue to see further protocol improvements by Microsoft for Kerberos, such as validating the new PAC_REQUESTOR structure across trusts (which should eliminate all non-existent user Golden Tickets) , verifying that memberships in the PAC are that of the resolved user, and maybe even verifying that information in the user profile is in the PAC and that the structure of the PAC is compliant. Having more native detections and preventions in place is never a bad thing and will help companies better defend themselves.

Joe Dibley
Security Researcher at Netwrix and member of the Netwrix Security Research Team. Joe is an expert in Active Directory, Windows, and a wide variety of enterprise software platforms and technologies, Joe researches new security risks, complex attack techniques, and associated mitigations and detections.