Unconstrained Delegation

blog.netwrix.com/2022/12/02/unconstrained-delegation

Joe Dibley

Unconstrained delegation represents a serious cybersecurity risk. By taking steps to abuse the Active Directory delegation controls applied to user and computer objects in an AD environment, an attacker can move laterally and even gain control of the domain.

Handpicked related content:
[Free Guide] Active Directory Delegation Best Practices

This blog post explores this area of attack (unconstrained delegation) and offers security teams and administrators effective strategies for mitigating this security risk.

What is unconstrained delegation?

Delegation enables a user or a computer to impersonate another account in order to access resources (such as back-end database servers). Delegation has several practical applications, which Microsoft covers in this blog post.

Using the Delegation tab on a user or computer account, you can configure either unconstrained or constrained delegation:

- By selecting “Trust this computer for delegation to any service (Kerberos delegation only),” you are enabling **unconstrained**
- Alternatively, you can restrict what services the user or computer can impersonate by specifying particular Service Principal Names (SPNs), which is **constrained** delegation**.**

Unconstrained Delegation 1

Note that another option is **resource-based constrained delegation** (RBCD), in which delegation is configured on the resource, rather than on the accounts accessing the resource. RBCD can be set up using Windows PowerShell.

What are the risks of unconstrained delegation?

Several attacks can be perpetrated against unconstrained delegation: some are covered in this blog post by harmj0y and Sean Metcalf describes others. Let's explore a couple.

Example 1: Abusing unconstrained delegation to compromise an entire AD forest

Security researchers have shown how an attacker who compromises a machine with unconstrained delegation in one forest can compromise another forest and every domain in it. If you have a two-way trust in place, an attacker can use the MS-RPRN printer bug to causes a DC to send authentication information back to the attacker, enabling them to use DCSync to compromise the trusted domain. For example, if your company acquired a small company and joined its domain to yours, an attacker who compromises a system in the small environment could take over your company's entire forest, which is definitely not good.

A KB article was released to provide a fix for this bug, and in Windows Server 2012 and up there is a security setting to prevent this, but it may **not** be switched on by default.

Example 2: Exploiting unconstrained delegation to enable lateral movement

Here’s another scenario. If unconstrained delegation is turned on for a computer, then any time an account connects to that computer, their ticket-granting ticket (TGT) from the Key Distribution Center (KDC) is stored in memory for later use by the computer. If the machine is compromised, the adversary can get that TGT and misuse it to do a great deal of damage — especially if the TGT is for a highly privileged user.

For example, suppose a Domain Admin accesses a particular computer over the Common Internet File System (CIFS) by accessing a shared folder. Without unconstrained delegation on, only the ticket-granting server (TGS) would be stored in memory; this ticket gives access only to the CIFS service on the local machine, so an adversary can’t use it to move laterally. We can see this using the Mimikatz command **sekurlsa::tickets /export**, which returns only the user’s service ticket (TGS):

However, if unconstrained delegation is enabled, the command returns the TGT for the admin account, which an adversary can use in a Pass-the-Ticket attack to compromise the entire domain.

Unconstrained Delegation 3

To harvest TGTs from any user who connects to the system, the adversary can use the following PowerSpoit command:

Unconstrained Delegation 4

Rights Required to Enable Unconstrained Delegation

To be able to manage the delegation controls of an object, a user needs the following rights:

- SeEnableDelegationPrivilege, a user right is controlled by the local security policyof a domain controller and managed through the Group Policy setting “Enable computer and user accounts to be trusted for delegation”, as illustrated below
- Ability to update the msDS-AllowedToDelegateTo and userAccountControl attributes for a computer, which is where this Group Policy setting is stored

Finding Unconstrained Delegation

To find out where unconstrained delegation has been enabled, you can use the following PowerShell script. It will check the User Account Control (UAC) value of all computers to see where delegation is turned on without restrictions.

You may also want to look at who has been granted the **SeEnableDelegationPrivilege** right. To do this, you can use PowerSploit and the Get-DomainPolicy command.

Best Practices for Reducing the Risk from Unconstrained Delegation

To reduce the risk from unconstrained delegation, it is recommended to:

- Investigate whether unconstrained delegation is actually required. In many cases, unconstrained delegation was mistakenly enabled and can be either disabled entirely or converted to constrained delegation or resource-based constrained delegation. *Keep in mind that it is not recommended to configure constrained delegation to a domain controller (DC), because an attacker who compromises a constrained delegation account will be able to impersonate any user to any service on the DC.*

- Use the “This account is sensitive and cannot be delegated” option to prevent sensitive accounts from being used in delegation.
- Place privileged users in the Protected Users group. This helps prevent them from being used in delegation and keeps their TGTs off the computer after they authenticate.
- Monitor the activity of delegated accounts closely. All systems where any type of delegation configured and used should be monitored for suspicious activity.

How can Netwrix help?

Unconstrained delegation is one of numerous attack vectors that malefactors can exploit to gain access to and create persistence in your Active Directory environment. With the Netwrix Active Directory Security Solution, you will able to:

- Discover security risks, including unneeded delegation, excessive permissions, standing privileges and GPO misconfigurations, and prioritize your mitigation efforts.
- Establish secure configurations across your entire IT infrastructure and maintain them by identifying and remediating any improper changes from your hardened baseline.
- Promptly detect and respond to advanced threats, such as Kerberoasting, DCSync, dit extraction and Golden Ticket attacks.
- Automate response to known attacks to minimize damage.
- Ensure fast recovery of Active Directory in the event of a security breach or other incident.

FAQ

What types of delegation are available in Active Directory?

There are 3 types of delegation that your organization can use:

- Unconstrained delegation
- Constrained delegation
- Resource-based constrained delegation (RBCD)

What is resource-based constrained delegation (RBCD)?

With RBCD, an administrator who owns a resource may delegate access to it.

How can I configure RBCD?

To configure a resource service to allow access on behalf of users, you can use Windows PowerShell cmdlets (**New-ADComputer**, **New-ADServiceAccount**, **New-ADUser**, **Set-ADComputer**, **Set-ADServiceAccount** and **Set-ADUser**) with the parameter **PrincipalsAllowedToDelegateToAccount**.

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.