Security Advisory 2021-077

Windows Domain Takeover Vulnerability

December 21, 2021 — v1.0

TLP:WHITE

History:

- *21/12/2021 — v1.0 – Initial publication*

Summary

During the November Patch Tuesday, Microsoft released a set of fixes for various vulnerabilities affecting several of its products [1]. On December 20th, Microsoft released a Security Advisory about two of these vulnerabilities (**CVE-2021-42287**, and **CVE-2021-42278**) which, when combined, could lead to Windows domain takeover [2]. Proofs-of-concept have been released publicly starting from December 11th.

Technical Details

CVE-2021-42278

Active Directory (AD) uses several naming schemes for a given object. Like `userPrincipalName` (UPN), and `sAMAccountName` (SAM-Account). In cases of computers – these `sAMAccountName` attributes usually end with `$` in their name. Traditionally, this `$` was used to distinguish between user objects and computer objects. It is important to mention there are no restrictions or validations for changing this attribute to include or not include the `$` character.

With default settings, when the relevant patch is not applied, a normal user has permissions to modify a machine account (up to 10 machines) and as its owner, he/she also has the permissions to edit its `sAMAccountName` attribute.

CVE-2021-42287

When performing an authentication using Kerberos, `Ticket-Granting-Ticket` (TGT) and the following `Ticket-Granting-Service` (TGS) are being requested from the Key Distribution Center (KDC). In case a TGS was requested for an account that could not be found, the KDC will attempt to search it again with a trailing `$`.

One could create a machine account, rename its SAM account name with the name of a Domain Controller without the trailing `$` and request a TGT. Then, the attacker could rename the SAM account name with a different name, and request a TGS ticket presenting the valid TGT.

When processing the TGS request, the KDC will fail its lookup for the requestor machine the attacker had created. Therefore, The KDC will perform another lookup appending a trailing `$`. The lookup will succeed. As a result, the KDC will issue the ticket using the privileges of the impersonated Domain Controller.

Attack Scenario

The combination of these two vulnerabilities could allow attackers to easily elevate their privilege to that of a Domain Admin once they compromise a regular user in the domain.

Affected products

- Windows Server 2012 R2 (Server Core Installation)
- Windows Server 2012 R2
- Windows Server 2012 (Server Core Installation)
- Windows Server 2012
- Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
- Windows Server 2008 R2 for x64-based Systems Service Pack 1
- Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
- Windows Server 2008 for x64-based Systems Service Pack 2
- Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
- Windows Server 2008 for 32-bit Systems Service Pack 2
- Windows Server 2016 (Server Core installation)
- Windows Server 2016
- Windows Server, version 20H2 (Server Core Installation)
- Windows Server, version 2004 (Server Core installation)
- Windows Server 2022 (Server Core installation)
- Windows Server 2022
- Windows Server 2019 (Server Core installation)
- Windows Server 2019

Recommendations

Microsoft and CERT-EU recommend patching the affected servers to prevent any compromise. Moreover, Security Analyst could look for possible past compromises [2].

Exploitation detection

Microsoft provides guidance to look for potential compromise by running Threat Hunting queries in Microsoft 365 Defender:

1. The sAMAccountName change is based on event 4662. Make sure to enable it on the domain controller to catch such activities [3].
2. Open Microsoft 365 Defender and navigate to Advanced Hunting.
3. Copy the following query (also available in the Microsoft 365 Defender GitHub Advanced Hunting query [4]):

```
IdentityDirectoryEvents
| where Timestamp > ago(1d)
| where ActionType == "SAM Account Name changed"
| extend FROMSAM = parse_json(AdditionalFields)['FROM SAM Account Name']
| extend TOSAM = parse_json(AdditionalFields)['TO SAM Account Name']
| where (FROMSAM has "$" and TOSAM !has "$")
        or TOSAM in ("DC1", "DC2", "DC3", "DC4") // DC Names in the org
| project Timestamp, Application, ActionType, TargetDeviceName, FROMSAM, TOSAM, ReportId,
  AdditionalFields
```

4. Replace the marked area with the naming convention of your domain controllers.
5. Run the query and analyse the results which contain the affected devices. You can use Windows Event 4741 to find the creator of these machines if they were newly created.
6. Investigate the compromised computers and determine that they haven't been weaponised.

References

[1] https://msrc.microsoft.com/update-guide/vulnerability

[2] https://techcommunity.microsoft.com/t5/security-compliance-and-identity/sam-name-impersonation/ba-p/3042699

[3] https://docs.microsoft.com/en-us/defender-for-identity/configure-windows-event-collection#configure-object-auditing

[4] https://github.com/microsoft/Microsoft-365-Defender-Hunting-Queries/blob/master/Privilege%20escalation/SAM-Name-Changes-CVE-2021-42278.md