Microsoft: May Windows updates cause AD authentication failures

Sergiu Gatlan

Microsoft is investigating a known issue causing authentication failures for some Windows services after installing updates released during the May 2022 Patch Tuesday.

This comes after Windows admins started sharing reports of some policies failing after installing this month's security updates with "Authentication failed due to a user credentials mismatch. Either the user name provided does not map to an existing account or the password was incorrect." errors.

The issue impacts client and server Windows platforms and systems running all Windows versions, including the latest available releases (Windows 11 and Windows Server 2022).

Microsoft says the known issue is only triggered after installing the updates on servers used as domain controllers. The updates will not negatively impact when deployed on client Windows devices and non-domain controller Windows Servers.

"After installing updates released May 10, 2022 on your domain controllers, you might see authentication failures on the server or client for services such as Network Policy Server (NPS), Routing and Remote access Service (RRAS), Radius, Extensible Authentication Protocol (EAP), and Protected Extensible Authentication Protocol (PEAP)," Microsoft explains.

"An issue has been found related to how the mapping of certificates to machine accounts is being handled by the domain controller."

Redmond is investigating this newly acknowledged issue and will provide an update addressing it in an upcoming release.

Caused by security updates, workaround available

Microsoft explains in a separate support document that these ongoing service authentication problems are caused by security updates addressing CVE-2022-26931 and CVE-2022-26923, two elevations of privilege vulnerabilities in Windows Kerberos and Active Directory Domain Services.

The more severe one, CVE-2022-26923 (discovered by security researcher Oliver Lyak and dubbed Certifried), can let attackers with access to a low privileged account elevate privileges to domain admin on default Active Directory configurations.

To address the known issue until an official update is available, Microsoft recommends manually mapping certificates to a machine account in Active Directory.

"If the preferred mitigation will not work in your environment, please see 'KB5014754—Certificate-based authentication changes on Windows domain controllers' for other possible mitigations in the *SChannel registry key* section," the company added.

"Any other mitigation except the preferred mitigations might lower or disable security hardening."

Microsoft says the May 2022 updates automatically set the StrongCertificateBindingEnforcement registry key, which changes the enforcement mode of the Kerberos Distribution Center (KDC) to Compatibility mode (and this should allow all auth attempts unless the certificate is older than the user).

However, a Windows admin told BleepingComputer that the only way to get some of their users to log in with this update was to disable the StrongCertificateBindingEnforcement key by setting it to 0.

If you don't find the key in the registry, create it from scratch using a REG_DWORD Data Type and set it to 0 to disable the strong certificate mapping check (although not recommended by Microsoft, it's the only way to allow all users to log in).

In November, Microsoft also addressed Windows Server authentication failures related to Kerberos delegation scenarios impacting Domain Controllers (DC) via out-of-band updates.