'Silver SAML' Haunts Entra ID Single Sign-On Security

Moving From AFDS to Avoid 'Golden SAML' Wasn't a Cure-All

BY Prajeet Nair (@prajeetspeaks) , David Perera (@daveperera) • February 29, 2024 (link)

The Russian intelligence hack against SolarWinds in 2020 had one unanticipated side effect: Enterprises rushed to replace on-premises single sign-on infrastructure with a cloud-native alternative.

They did so because once the SolarWinds supply chain hack gave Moscow hackers a toehold into victim networks, they stole the certificates from Active Directory Federation Services servers, allowing them to sign onto services such as Outlook without having to crack a password. They used an attack known as Golden SAML because the attack manipulates the Security Assertion Markup Language messages that service providers use to authenticate users.

Just like most users, Russian hackers saw the advantage of single sign-on: convenience and access to many services without the bother of multiple passwords. Unfortunately for system administrators, the other side of the bargain - reduced attack surface - didn't apply. Hence a rush to ditch ADFS for a new, cloud-native way to manage single sign-on authentication: Microsoft Azure AD, now known as Entra ID.

But the story doesn't stop there, say researchers from Semperis, who detail how attackers can execute an attack similar to Golden SAML in an Entra ID environment. Researchers could have called the new attack - which so far is apparently just theoretical - "Child of Golden SAML," but Semperis went with "Silver SAML."

"When SolarWinds hit and the fallout happened, the message at a high level was, 'If you just move to Entra, Golden SAML can never happen,'" Semperis researcher Eric Woodruff told Information Security Media Group. "But these organizations that have bad habits could still set themselves up to have a [Silver] SAML attack."

Silver SAML exploits a vulnerability common in Entra ID single sign-on environments. Under ordinary circumstances, a user logs on to a service provider such as Salesforce or Workday, which sends Entra ID a SAML request - which prompts Entra ID to authenticate the user. When that is done, Entra ID sends a SAML response to the service provider and the user gains access.

With a SilverSAML attack, an attacker could swipe the private key used to sign the SAML response to craft forged SAML responses. In worst-case scenarios, the attacker could use the private key to logon to a service provider without the service first contacting Entra ID.

Private keys are vulnerable because many organizations think it's a best practice to obtain certificates from an outside party. That triggers private key management issues not helped by the way many firms handle certificates - such as keeping them in a folder labeled "certificates."

"The behavior is very similar to if my desktop had a folder that said 'passwords,'" Woodruff said.

Semperis recommends organization head off Silver SAML attacks by only using Entra ID self-signed certificates for single sign-on. In contrast with third-party certificates, "Microsoft can take a shortcut, because they own the whole stack. They can insert it wherever it needs to go, but you don't need to have it in your hands, which is the big difference."

The company also says switching to OpenID Connect - an authentication protocol based on the OAuth 2.0 framework - for authentication is a possibility.

Alternatively, Woodruff said, service developers can add an additional layer of security to SAML requests by validating the signature of signed authentication requests, a technique that Microsoft calls SAML Request Signature Verification.

There are tradeoffs, Woodruff said: It might limit the ease of single sign-on. But the main limitation is that most service providers haven't implemented signature verification, he said. "It's not even an option in a lot of applications."

Semperis researchers developed a proof-of-concept tool called SilverSAMLForger that can be used to forge signed SAML responses.