Detecting Abuse of Authentication Mechanisms

Summary

Malicious cyber actors are abusing trust in federated authentication environments to access protected data. The exploitation occurs after the actors have gained initial access to a victim's on-premises network. The actors leverage privileged access in the on-premises environment to subvert the mechanisms that the organization uses to grant access to cloud and on-premises resources and/or to compromise administrator credentials with the ability to manage cloud resources. The actors demonstrate two sets of tactics, techniques, and procedures (TTP) for gaining access to the victim network's cloud resources, often with a particular focus on organizational email.

In the first TTP, the actors compromise on-premises components of a federated SSO infrastructure and steal the credential or private key that is used to sign Security Assertion Markup Language (SAML) tokens (TA0006[1], T1552, T1552.004). Using the private keys, the actors then forge trusted authentication tokens to access cloud resources. A recent NSA Cybersecurity Advisory warned of actors exploiting a vulnerability in VMware Access®[2] and VMware Identity Manager®[3] that allowed them to perform this TTP and abuse federated SSO infrastructure [1]. While that example of this TTP may have previously been attributed to nation-state actors, a wealth of actors could be leveraging this TTP for their objectives. This SAML forgery technique has been known and used by cyber actors since at least 2017 [2].

In a variation of the first TTP, if the malicious cyber actors are unable to obtain an on-premises signing key, they would attempt to gain sufficient administrative privileges within the cloud tenant to add a malicious certificate trust relationship for forging SAML tokens.

In the second TTP, the actors leverage a compromised global administrator account to assign credentials to cloud application service principals (identities for cloud applications that allow the applications to be invoked to access other cloud resources). The actors then invoke the application's credentials for automated access to cloud resources (often email in particular) that would otherwise be difficult for the actors to access or would more easily be noticed as suspicious (T1114, T1114.002).

Note that these TTPs (in and of themselves) do not constitute vulnerabilities in the design principles of federated identity management, the SAML protocol, or on-premises and cloud identity services. The security of identity federation in any cloud environment directly depends on trust in the on-premises components that perform authentication, assign privileges, and sign SAML tokens. If any of these components is compromised, then the trust in authentication tokens from the components is misplaced and can be abused for unauthorized access.

It is critical when running products that perform authentication that the server and all the services that depend on it are properly configured for secure operation and integration. Otherwise, SAML tokens could be forged, granting access to numerous resources. Microsoft Active Directory Federation Services (ADFS) ®[4] is an identity federation technology used to federate identities with Active Directory (AD) ®[5], Azure Active Directory (AAD) ®[6], and other identity providers, such as VMware Identity Manager. By abusing the federated authentication, the actors are not exploiting a vulnerability in ADFS, AD, or AAD, but rather abusing the trust established across the integrated components. Due to the popularity of ADFS, numerous actors target ADFS, as well as other identity providers trusted by ADFS (T1199), to gain access to cloud services, such as Microsoft Office 365. Once access is gained, the actors monitor or exfiltrate emails and documents

[1] TA0006 and similar references are MITRE® ATT&CK® tactics and techniques. MITRE and ATT&CK are registered trademarks of The MITRE Corporation.
[2] VMware Access ® is a registered trademark of VMware.
[3] VMware Identity Manager ® is a registered trademark of VMware.
[4] Microsoft Active Directory Federation Services (ADFS) ® is a registered trademark of Microsoft Corporation.
[5] Active Directory (AD) ® is a registered trademark of Microsoft Corporation.
[6] Azure Active Directory (AAD) ® is a registered trademark of Microsoft Corporation.

stored in Microsoft Office 365®[7] environments (T1114, T1114.002). Therefore, when using ADFS, NSA recommends following Microsoft's®[8] best practices, especially for securing SAML tokens and requiring multi-factor authentication [3] [4].

Regardless of how the initial on-premises compromise occurred, detecting authentication abuse can aid in detecting the compromise and even contain it if responded to quickly enough. The recent SolarWinds Orion®[9] code compromise is one serious example of how on-premises systems can be compromised leading to abuse of federated authentication and malicious cloud access [5] [6]. Affected customers are strongly recommended to follow CISA's Emergency Directive 20-01 to perform incident response and take mitigation actions [7].

Mitigation Actions

To defend against these TTPs, cloud tenants must pay careful attention to locking down tenant SSO configuration and service principal usage, as well as hardening the systems that run on-premises identity and federation services. Monitoring the use of SSO tokens and the use of service principals in the cloud can help detect the compromise of identity services. While these techniques apply to all cloud environments that support on-premises federated authentication, the following specific mitigations are focused on Microsoft Azure federation. Many of the techniques can be generalized to other environments.

Harden Azure Authentication and Authorization Configuration

Azure tenants can configure aspects of authentication and authorization in Azure Active Directory (AAD). When possible, AAD should be configured to reject authorization requests with tokens having characteristics that deviate from common practices.

- Refer to Microsoft guidance on securing privileged access [8] [9] [10] [11];
- Token claims should be consistent with organizational policy;

Azure tenants should follow basic security practices on locking down the use of service principals:

- Review all tenant applications with credentials and remove if not necessary;

Follow recommended AAD security practices.

- Refer to Microsoft guidance on requiring and enforcing Multi-Factor Authentication (MFA) [12] [13] [14];
- Refer to Microsoft guidance on disabling legacy authentication to AAD [15].

Harden On-Premises Systems

The ability of actors to conduct this attack hinges on the initial compromise of customer on-premises systems. Without administrative access to the on-premises identity provider, actors would not be able to generate tokens for use in the cloud. Follow NSA guidance on locking down endpoint systems, beginning with keeping systems patched and software updated [20].

Strongly consider deploying a FIPS validated Hardware Security Module (HSM) to store on-premises token signing certificate private keys. An HSM, aggressively updated, makes it very difficult for actors who have compromised the system to steal the private keys and use them outside of the network [3].

Ensure core privileged cloud administrative users, groups, and roles are not impacted by data synchronized from on-premises environments, and that cloud administrative roles do not authenticate with SMAL SSO, but instead rely on cloud-only authentication.

[7] Microsoft Office 365® is a registered trademark of Microsoft Corporation.
[8] Microsoft® is a registered trademark of Microsoft Corporation.
[9] SolarWinds Orion ® is a registered trademark of SolarWinds Worldwide LCC.

Detection

Detecting forged SAML token usage is a shared responsibility between the cloud provider and tenant. The cloud provider leverages its position to look for sophisticated attacks against customers, while the tenant can detect indications in both on-premises and cloud logs. For this reason it is important to inspect and retain your logs for analysis.

When available, utilize add-on cloud services and log correlation tools that use environmental values and sophisticated AI/ML algorithms to detect unusual patterns in user authentication and authorization. For those organizations using the Azure cloud®[10], Microsoft offers tools including Azure AD Identity Protection®[11], Microsoft Cloud Application Security®[12], and Azure Sentinel, but other third-party products may be used to perform log analysis as well. [16] [17].

Examine logs for suspicious tokens that do not match the baseline for SAML tokens that are typical for the tenant, and audit SAML token use to detect anomalies, for example:

- Tokens with an unusually long lifetime;
- Tokens with unusual claims that do not match organizational policy;
- Tokens that claim to have been authenticated using a method that is not used by the organization (e.g., MFA when the organization does not use MFA, or MFA by a provider that does not usually perform MFA);
- Tokens presented without corresponding log entries, such as tokens with MFA claims where there is no corresponding MFA system transaction, or tokens consumed at the resource with no corresponding federation server transaction.
- Tokens that include a claim that it is for inside the corporate network when it is not;
- Tokens that are used to access cloud resources that do not have records of being created by the on-premises identity provider in its logs

Examine logs for the suspicious use of service principals:

- Audit the creation and use of service principal credentials;
- In particular, look for unusual application usage, such as a dormant or forgotten application being used again;
- Audit the assignment of credentials to applications that allows non-interactive sign-in by the application [18] [19].

Look for unexpected trust relationships that have been added to AAD [18].

Consider using Azure Active Directory as the Authoritative Identity Provider

By consolidating identity and access natively in the cloud, tenants relieve themselves from the burden of managing the federation of authentication and the on-premises service, and gain more of the protections that the cloud provider has in place, including system hardening, configuration and monitoring. The drawback of doing this is that SSO may not work across on-premises and cloud resources and the tenant must trust the cloud provider to host user credential information.

[10] Azure cloud ® is a registered trademark of Microsoft Corporation.
[11] Azure AD Identity Protection ® is a registered trademark of Microsoft Corporation.
[12] Microsoft Cloud Application Security ® is a registered trademark of Microsoft Corporation.

Works Cited

[1] NSA, "Russian State-Sponsored Actors Exploiting Vulnerability in VMware® Workspace ONE Access Using Compromised Credentials," NSA, 7 Dec 2020. [Online]. Available: https://media.defense.gov/2020/Dec/07/2002547071/-1/-1/0/CSA_VMWARE%20ACCESS_U_OO_195976_20.PDF. [Accessed 11 Dec 2020].

[2] S. Reiner, "Golden SAML: Newly Discovered Attack Technique Forges Authentication to Cloud Apps," CyberArk, 21 Nov 2017. [Online]. Available: https://www.cyberark.com/resources/threat-research-blog/golden-saml-newly-discovered-attack-technique-forges-authentication-to-cloud-apps. [Accessed 11 Dec 2020].

[3] Microsoft, "Best practices for securing Active Directory Federation Services," Microsoft, 31 May 2017. [Online]. Available: https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/deployment/best-practices-securing-ad-fs. [Accessed 9 Dec 2020].

[4] Microsoft, "Best Practices for Secure Planning and Deployment of AD FS," Microsoft, 31 May 2017. [Online]. Available: https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/design/best-practices-for-secure-planning-and-deployment-of-ad-fs. [Accessed 9 Dec 2020].

[5] L. SolarWinds Worldwide, "SolarWinds Security Advisory," 15 December 2020. [Online]. Available: https://www.solarwinds.com/securityadvisory. [Accessed 15 December 2020].

[6] M. S. R. Center, "Customer Guidance on Recent Nation-State Cyber Attacks," 13 December 2020. [Online]. Available: https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/. [Accessed 15 December 2020].

[7] Cybersecurity and Infrastructure Security Agency, "Emergency Directive 21-01: Mitigate SolarWinds Orion Code Compromise," 13 December 2020. [Online]. Available: https://cyber.dhs.gov/ed/21-01/. [Accessed 15 December 2020].

[8] Microsoft, "Securing privileged access for hybrid and cloud deployments in Azure AD," Microsoft, 5 Nov 2020. [Online]. Available: https://docs.microsoft.com/en-us/azure/active-directory/roles/security-planning. [Accessed 11 Dec 2020].

[9] Microsoft, "Securing privileged access," Microsoft, 25 Feb 2019. [Online]. Available: https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access. [Accessed 11 Dec 2020].

[10] Microsoft, "Privileged Access Workstations," Microsoft, 13 Mar 2019. [Online]. Available: https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/privileged-access-workstations. [Accessed 11 Dec 2020].

[11] Microsoft, "Active Directory administrative tier model," Microsoft, 14 Feb 2019. [Online]. Available: https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material. [Accessed 11 Dec 2020].

[12] Microsoft, "Conditional Access: Require MFA for Azure management," Microsoft, 26 May 2020. [Online]. Available: https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-azure-management. [Accessed 9 Dec 2020].

[13] Microsoft, "Conditional Access: Require MFA for administrators," Microsoft, 3 Aug 2020. [Online]. Available: https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-admin-mfa. [Accessed 9 Dec 2020].

[14] Microsoft, "Conditional Access: Require MFA for all users," Microsoft, 26 May 2020. [Online]. Available: https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-all-users-mfa. [Accessed 9 Dec 2020].

[15] Microsoft, "How to: Block legacy authentication to Azure AD with Conditional Access," Microsoft, 5 Nov 2020. [Online]. Available: https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/block-legacy-authentication. [Accessed 9 Dec 2020].

[16] Microsoft, "How to investigate anomaly detection alerts," Microsoft, 8 June 2020. [Online]. Available: https://docs.microsoft.com/en-us/cloud-app-security/investigate-anomaly-alerts. [Accessed 11 Dec 2020].

[17] Microsoft, "Alert policies in the security and compliance center," Microsoft, 19 Nov 2020. [Online]. Available: https://docs.microsoft.com/en-us/microsoft-365/compliance/alert-policies?view=o365-worldwide. [Accessed 11 Dec 2020].

[18] Microsoft Security Response Center, "Customer Guidance on Recent Nation-State Cyber Attacks," Microsoft, 13 Dec 2020. [Online]. Available: https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/. [Accessed 14 Dec 2020].

[19] N. Carr and shainw, "Azure/Azure-Sentinel/Detections/AuditLogs/NewAppOrServicePrincipalCredential.yaml," 3 Dec 2020. [Online]. Available: https://github.com/Azure/Azure-Sentinel/blob/master/Detections/AuditLogs/NewAppOrServicePrincipalCredential.yaml. [Accessed 15 Dec 2020].

[20] NSA, "UPDATE AND UPGRADE SOFTWARE IMMEDIATELY," NSA, 30 Aug 2019. [Online]. Available: https://media.defense.gov/2019/Sep/09/2002180319/-1/-1/0/UPDATE%20AND%20UPGRADE%20SOFTWARE%20IMMEDIATELY.PDF. [Accessed 9 Dec 2020].

Disclaimer of Endorsement

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

Purpose

This document was developed in furtherance of NSA's cybersecurity missions, including its responsibilities to identify and disseminate threats to National Security Systems, Department of Defense, and Defense Industrial Base information systems, and to develop and issue cybersecurity specifications and mitigations. This information may be shared broadly to reach all appropriate stakeholders.

Contact

Client Requirements / General Cybersecurity Inquiries: Cybersecurity Requirements Center, 410-854-4200, Cybersecurity_Requests@nsa.gov
Media inquiries / Press Desk: Media Relations, 443-634-0721, MediaRelations@nsa.gov