National Security Agency | Cybersecurity Advisory

Detecting Abuse of Authentication Mechanisms - Abridged

Summary

Malicious cyber actors are abusing trust in federated authentication environments to access protected data. An “on premises” federated identity provider or single sign-on (SSO) system lets an organization use the authentication systems they already own (e.g. tokens, authentication apps, one-time passwords, etc.) to grant access to resources, including resources in “off premises” cloud services. These systems often use cryptographically signed automated messages called “assertions” shared via Security Assertion Markup Language (SAML) to show that users have been authenticated. When an actor can subvert authentication mechanisms, they can gain illicit access to a wide range of an organizations assets.

In some cases, actors have stolen keys from the SSO system that allow them to sign assertions and impersonate any legitimate user who could be authenticated by the system. On 7 December, NSA reported on an example where a zero-day vulnerability was being used to compromise VMware Access®[1] and VMware Identity Manager®[2] servers, allowing actors to forge authentication assertions and thus gain access to the victim’s protected data. In other cases, actors have gained enough privileges to create their own keys and identities such as “service principals” (cloud applications that act on behalf of a user) or even their own fake SSO system. According to public reporting, in some cases, the SolarWinds Orion®[3] code compromise provided actors initial access to an on-premises network which led to access within the cloud.

Note that these techniques alone 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 the federated identity system can be abused for unauthorized access.

To defend against these techniques, organizations should pay careful attention to locking down 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®[4] federation. Many of the techniques can be generalized to other environments as well.

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

[1]. VMware Access is a registered trademark of VMware
[2]. VMware Identity Manager is a registered trademark of VMware
[3] SolarWinds Orion ® is a registered trademark of SolarWinds Worldwide LCC.
[4] Azure ® is a registered trademark of Microsoft Corporation.