Results of Major Technical Investigations for Storm-0558 Key Acquisition

MSRC / By MSRC / September 06, 2023 / 3 min read

On July 11, 2023, Microsoft published a blog post which details how the China-Based threat actor, Storm-0558, used an acquired Microsoft account (MSA) consumer key to forge tokens to access OWA and Outlook.com. Upon identifying that the threat actor had acquired the consumer key, Microsoft performed a comprehensive technical investigation into the acquisition of the Microsoft account consumer signing key, including how it was used to access enterprise email. Our technical investigation has concluded. As part of our commitment to transparency and trust, we are releasing our investigation findings.

Key acquisition

Microsoft maintains a highly isolated and restricted production environment. Controls for Microsoft employee access to production infrastructure include background checks, dedicated accounts, secure access workstations, and multi-factor authentication using hardware token devices. Controls in this environment also prevent the use of email, conferencing, web research and other collaboration tools which can lead to common account compromise vectors such as malware infections or phishing, as well as restricting access to systems and data using Just in Time and Just Enough Access policies.

Our corporate environment, which also requires secure authentication and secure devices, allows for email, conferencing, web research and other collaboration tools. While these tools are important, they also make users vulnerable to spear phishing, token stealing malware, and other account compromise vectors. For this reason - by policy and as part of our Zero-Trust and "assume breach" mindset - key material should not leave our production environment.

Our investigation found that a consumer signing system crash in April of 2021 resulted in a snapshot of the crashed process ("crash dump"). The crash dumps, which redact sensitive information, should not include the signing key. In this case, a race condition allowed the key to be present in the crash dump (this issue has been corrected). The key material's presence in the crash dump was not detected by our systems (this issue has been corrected).

We found that this crash dump, believed at the time not to contain key material, was subsequently moved from the isolated production network into our debugging environment on the internet connected corporate network. This is consistent with our standard debugging processes. Our credential scanning methods did not detect its presence (this issue has been corrected).

After April 2021, when the key was leaked to the corporate environment in the crash dump, the Storm-0558 actor was able to successfully compromise a Microsoft engineer's corporate account. This account had access to the debugging environment containing the crash dump which incorrectly contained the key. Due to log retention policies, we don't have logs with specific evidence of this exfiltration by this actor, but this was the most probable mechanism by which the actor acquired the key.

Why a consumer key was able to access enterprise mail

To meet growing customer demand to support applications which work with both consumer and enterprise applications, Microsoft introduced a common key metadata publishing endpoint in September 2018. As part of this converged offering, Microsoft updated documentation to clarify the requirements for key scope validation – which key to use for enterprise accounts, and which to use for consumer accounts.

As part of a pre-existing library of documentation and helper APIs, Microsoft provided an API to help validate the signatures cryptographically but did not update these libraries to perform this scope validation automatically (this issue has been corrected). The mail systems were updated to use the common metadata endpoint in 2022. Developers in the mail system incorrectly assumed libraries performed complete validation and did not add the required issuer/scope validation. Thus, the mail system would accept a request for enterprise email using a security token signed with the consumer key (this issue has been corrected using the updated libraries).

Post Incident Review

Microsoft is continuously hardening systems as part of our defense in depth strategy. Investments which have been made related to MSA key management are covered in the https://aka.ms/storm-0558 blog. Items detailed in this blog are a subset of these overall investments. We are summarizing the improvements specific to these findings here for clarity:

1. Identified and resolved race Condition that allowed the signing key to be present in crash dumps
2. Enhanced prevention, detection, and response for key material erroneously included in crash dumps
3. Enhanced credential scanning to better detect presence of signing key in the debugging environment
4. Released enhanced libraries to automate key scope validation in authentication libraries, and clarified related documentation

Azure AD   Identity   Investigations

< Previous Post   Next Post >

Related Posts

- Storm-0558 によるキーの取得に関する主な技術調査の結果について
- Azure AD アプリケーションにおける特権昇格の潜在的なリスクについて
- Potential Risk of Privilege Escalation in Azure AD Applications

Search blog posts

Subscribe

Categories

MSRC (1052)

Japan Security Team (1012)

Security Research & Defense (378)

BlueHat (188)

Microsoft Threat Hunting (4)

Bug Bounty Programs (2)

Security Research (1)

Tags

セキュリティ情報 (464)

脆弱性 (248)

アドバイザリ (171)

Internet Explorer (IE) (156)

Security Update (140)

Security Advisory (134)

Security Bulletin (133)

Mitigations (128)

Community-based Defense (106)

Microsoft Windows (106)

View all Tags

Recent Posts

Introducing the Microsoft AI Bug Bounty Program featuring the AI-powered Bing experience

Microsoft Response to Distributed Denial of Service (DDoS) Attacks against HTTP/2

Cybersecurity Awareness Month 2023: Elevating Security Together

Microsoft's Response to Open-Source Vulnerabilities - CVE-2023-4863 and CVE-2023-5217

Journey Down Under: How Rocco Became Australia's Premier Hacker

Archives

October 2023 (8)

September 2023 (6)

August 2023 (9)

July 2023 (10)

June 2023 (9)

View full Archive

What's new

Surface Pro 9

Surface Laptop 5

Surface Studio 2+

Surface Laptop Go 2

Surface Laptop Studio

Surface Go 3

Microsoft 365

Windows 11 apps

Microsoft Store

Account profile

Download Center

Microsoft Store support

Returns

Order tracking

Trade-in for Cash

Microsoft Store Promise

Flexible Payments

Education

Microsoft in education

Devices for education

Microsoft Teams for Education

Microsoft 365 Education

How to buy for your school

Educator training and development

Deals for students and parents

Azure for students

Business

Microsoft Cloud

Microsoft Security

Dynamics 365

Microsoft 365

Microsoft Power Platform

Microsoft Teams

Microsoft Industry

Small Business

Developer & IT

Azure

Developer Center

Documentation

Microsoft Learn

Microsoft Tech Community

Azure Marketplace

AppSource

Visual Studio

Company

Careers

About Microsoft

Company news

Privacy at Microsoft

Investors

Diversity and inclusion

Accessibility

Sustainability

English (United States)

Your Privacy Choices

Sitemap Contact Microsoft Privacy Terms of use Trademarks Safety & eco Recycling About our ads © Microsoft 2023