Microsoft

Updates on Microsoft's Secure Future Initiative (SFI) progress

May 1, 2024

In addition to the SFI progress outlined in the March blog from Microsoft Corporate Vice President and Chief Cybersecurity Advisor Bret Arsenault, Microsoft accelerated SFI engineering work further in response to the Midnight Blizzard attack, with thousands of engineers being redeployed across the company, and the direct engagement of senior leadership in status updates twice a week or more. While we have more to do in fully implementing the SFI roadmap Brad Smith, Charlie Bell, Rajesh Jha and Scott Guthrie laid out in November 2023, learnings from our accelerated work countering Midnight Blizzard are raising the security bar and helping execute our SFI vision.

In the course of responding to the Midnight Blizzard's attack, Microsoft's teams accelerated progress on a number of initiatives, including:

- Accelerated lifecycle management of tenants focusing on unused or aged systems, which often have legacy configurations and can be targets for attacks, by proactively **removing more than 1.7 million Entra ID systems related to unused, aged or legacy configurations.**
- Raised the bar on securing tenants by default, by changing multi-factor authentication (MFA) defaults from being required by policy to automatically enforced with no human interaction necessary. We have implemented this **automatic enforcement of MFA across more than 1 million Entra ID tenants** within Microsoft, including tenants for development, testing, demos and production.
- Eliminated or reduced application targets by **removing 730,000 apps to-date across production and corporate tenants that were out-of-lifecycle or not meeting current SFI standards.**
- **Added additional security layers for creating digital identities across Microsoft, including mandatory video calls between managers and employees/vendors,** and the issuance of short-lived credentials directly to new employee/vendors to make impersonation and theft of credentials much harder. This is now implemented for more than 270,000 employees and vendors.
- **Enhanced the security of our own MFA implementation** with Microsoft Authenticator, by removing the call feature, where employees validate a login attempt via a phone call. We decided that simple in-app login prompting was preferable and more secure than using telecom infrastructure. **We accelerated that change across our enterprise, today covering more than 300,000 Microsoft employees and vendors.** This is like when we removed SMS authentication a decade ago and is another example of tangible security changes experienced daily at the company.

Microsoft

- **Integrated more scanning technologies to simultaneously look for the presence of more types of what we call "secrets"—think of credentials, certificates, and other sensitive information—in this traffic, to spot suspicious patterns and transit, in addition to verifying identity.** In a physical analogy, this is akin to looking beyond the vehicle and driver IDs on a secure facility's grounds, to also verify "what" these vehicles are carrying and "where" they're headed, even within the site's secure perimeter.

- Strengthened security further by ensuring that **administrators themselves adding tenants cannot remove or alter MFA enforced settings.**

- Because attackers prize creating—or hijacking and abusing—access controls, we've **increased our ability to remove detected user access violations in near real-time across Microsoft-owned services.** This advances our Zero Trust capabilities even further to cut off attacks compromising an identity, device, or other entry vector.

- Out of an abundance of caution, **we've proactively rotated 98% of our production application credentials,** and will be at 100% very quickly.

- Changed how we handle and track certificates internally because sophisticated attackers seek to create or steal and weaponize certificates. **To thwart these attacks, today we handle certificates in a more compartmentalized fashion, to prevent certificates from being used across tenants.**

- To further protect Microsoft's IT infrastructure supporting identity services, we have implemented **more network controls** to improve defense-in-depth. For example, our management systems handling keys and tokens for our own employees are now protected by both strict identity and network access control and are locked down to only accept connections from Microsoft IP ranges.

- On April 9, we announced a significant shift on our response process: We are now publishing root cause data for Microsoft CVEs (vulnerabilities) using the Common Weakness Enumeration (CWE) industry standard. CWE is a community-developed list of common software and hardware weaknesses that helps to **eliminate a whole class of vulnerabilities rather than individual vulnerabilities**. This work is a meaningful step toward a more cyber-secure world and **core to improving transparency and faster vulnerability responses.** Moving to this standards-based approach simplifies working with the entire security community including researchers, customers and partners.

SFI is an ongoing effort, and we will continue to make progress and share updates as we go forward.