Microsoft

Setting a new standard for faster vulnerability response and security updates

By Aanchal Gupta

The cyber threat landscape is evolving at an unprecedented pace. And new technologies like AI are fueling attacker innovation even as they unlock greater productivity gains for security teams. The industry is at an inflection point that requires a dramatic new approach to security, particularly vulnerability response. With relentless and sophisticated cyberattacks launched by countries and criminals on a daily basis, the industry needs vulnerability responses that are as fast and as intricate as the attacks we face.

The Microsoft Security Response Center (MSRC), which leads vulnerability response, has over two decades of experience partnering with the greater cybersecurity community to detect and respond to the latest vulnerabilities. But just as the threat landscape is always changing, so must our defense strategies.

To respond to the challenges we're seeing in today's threat landscape, Microsoft has introduced the Secure Future Initiative. A multi-year commitment to advance the way we design, build, test, and operate our technology, the Secure Future Initiative was created to ensure we deliver solutions that meet the highest possible standard of security.

One of the initial actions we are taking as part of this initiative is setting a new standard for faster vulnerability response and security updates, as well as greater transparency. In this paper, we will show you Microsoft's vulnerability response processes and partnership policies that will help us achieve our goals and hold ourselves accountable.

Accelerating our vulnerability response

A new goal for remediation development and deployment

We're committed to delivering updates with the speed and reliability our customers need to address threats head-on in today's shifting cyber threat landscape.

Microsoft's new goal for mitigating cloud vulnerabilities is a 50% reduction in time from confirmation of a vulnerability to a fix, compared to the current approach. Our goal is to continue to provide customers with comprehensive mitigations as quickly as possible when a new threat appears.

No NDAs for vulnerability disclosures

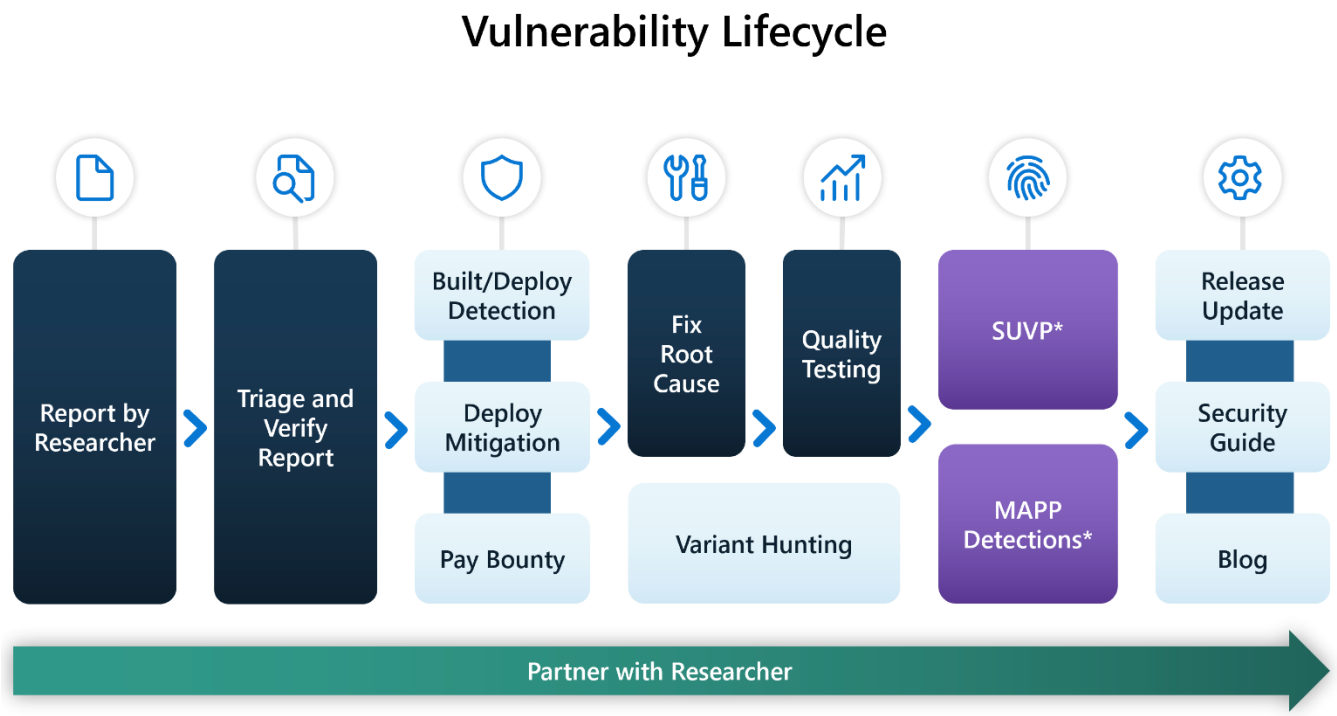
One of the ways in which we've led the charge in security response over the years is our no-NDA policy for third-party security researchers. We don't want to deter further research into any security issues that are reported to us, and we want to ensure that our customers have all the facts about a given situation. That's why we continue to welcome our security research partners' publication and discussion of their findings on any known security issues. As part of that community building, Microsoft practices Coordinated Vulnerability Disclosure (CVD). CVD is a standard of collaboration between vendors and researchers, giving vendors the opportunity to mitigate vulnerabilities before they become widely exploited and providing affected customers with timely and consistent guidance.

We understand that our stance against NDAs in vulnerability disclosure may have led to a perception that Microsoft experiences "more" vulnerabilities than our peers. But we are dedicated to following the CVD process because we know that's the best way to protect our customers and provide the right level of disclosure. We hope that our continued commitment to this principle will lead the way for our industry partners and encourage them to do the same.

Rigorous processes for fixing vulnerabilities

Customer trust and safety is paramount for us. To ensure that mitigations are developed in a way that preserves customer trust, safety, and functionality while addressing all possible angles of an attack, the MSRC works in several stages. We have iterated on our vulnerability response process for over two decades, in partnership with the security community.

The process begins with an initial report by a researcher and spans all the way through to a released update, for vulnerabilities in both cloud and on-premises products and services. Our well-established process is designed for both speed and quality to ensure that effective fixes are delivered in a timely manner. Please note that while this is the normal process we follow for remediating vulnerabilities, there may be exceptions for select cases.



*Applies only to on-premises vulnerabilities

First, a report comes in from a researcher through our Researcher Portal. The portal ensures fast and easy collaboration between researchers and the MSRC for all the information necessary to reproduce the issue, respond to the report, and fix the vulnerabilities behind it.

Once the report is submitted, the MSRC team triages and verifies the vulnerability. Researchers sometimes aren't sure of the full impact of the issue they are reporting, which is what our team assesses during this stage. As part of vulnerability verification, a security engineer assesses details and reproduces the issue. In some cases, the MSRC team may reach out to the security researcher reporting the issue for additional information regarding the configuration, environment, and other details to correctly reproduce the issue reported and evaluate the severity and security impact so that the case can move to the next stage without any delays. The product engineering team then focuses on building and deploying detections. Detections help us monitor any exploit in the wild and are early indicators to pivot if the vulnerability is broadly known and exploited. The team may also build mitigations, which can help break the exploit in a tactical way that helps protect

customers while a more permanent fix is developed. For the best researcher experience, it's also at this stage that they will be paid a bounty if the issue reported is covered under the program.

Then the engineering team works to fix the root cause with a deeper solution and performs multiple rounds of quality testing to ensure that the fix will not disrupt any customer operations. In parallel, the MSRC team hunts for any variants that would get past the proposed fix. We do this to ensure our released update thoroughly defends against any potential threats aimed at the vulnerability. We'd rather fix the problem once the right way than rush an update out that breaks our customers' systems and damages the trust in our solutions.

Once the fix is developed and tested to meet our rigorous standards, we release it. For cloud vulnerabilities, the fix is immediately released to the public. For vulnerabilities related to on-premises products, we first release the details to select external parties through two programs where information is shared with customers ahead of time. Participants of the Security Update Validation Program (SUVP) receive the update ahead of its full release, so that we can further test that the fix does not break the customers' normal workflows and that all product functionality is working as expected. Meanwhile, security software providers participating in the Microsoft Active Protections Program (MAPP) also receive information about high-risk vulnerabilities ahead of time to help them more quickly provide protections through their security products. That way, customers will be protected from the vulnerability even if they don't immediately update upon the monthly release.

While cloud fixes are delivered immediately, the MSRC generally releases security updates for on-premises products on Patch Tuesday, the second Tuesday of each month, so that IT professionals can properly plan their deployments. In case of extremely critical issues, MSRC releases immediate updates outside of the Patch Tuesday schedule.

Security updates for both on-premises fixes and some cloud fixes are posted to the Security Update Guide, which includes information such as the products affected, the impact and severity of the issue, the release notes, and Common Vulnerabilities and Exposure (CVE) details. The MSRC team also publishes regular blogs on known issues for both cloud and on-premises products on the Microsoft Security Response Center Blog to keep communication open regarding results of investigations and released updates. Customers can subscribe to Security Update Guide notifications to read further details on releases of security updates. Once the update has been released, the researchers involved in reporting the issues can discuss their findings with the wider public as well to further awareness and education.

As you can see, acceleration is built into every step of our vulnerability response strategy, while striking the delicate balance of addressing each issue in its entirety and ensuring high quality. While we feel that this process and the team of external researchers and internal security experts and engineering talent will help us achieve the fastest security update development time in the industry, we welcome feedback on areas where we can continue to accelerate.

Partnering with the security community on vulnerability discovery

At MSRC, we know that security isn't just about finding bugs and fixing them. It's about building a community that is focused on the same goal: honing our security skills so that we remain on the cutting edge of cyber defense. Security researchers make vital contributions to enhancing the security of our products, impacting over a billion customers.

The dynamic nature of the cloud demands security defenders must work together to protect customers from the onslaught of attacks. Microsoft has built a community of over 10,000 security and threat intelligence experts who are constantly focused on vulnerability discovery, understanding attack trends, and addressing patterns of security issues.

Recognizing the contributions of researchers

As part of our community-building efforts, we incentivize researchers through the Microsoft Bug Bounty Program. Approaching its 10-year anniversary, our bug bounty program is one of the most proactive in the industry.

We've always taken a leading approach with our security programs, and that includes the bug bounty program. After seeing an uptick in externally reported vulnerabilities impacting several cloud providers, we were the first in the industry to include cloud services in our bounty program. We furthered that approach by including higher rewards for cross-tenant bug reports starting in 2021. And in 2023, we announced the new Microsoft AI bug bounty program, which comes as a result of key investments and learnings on AI security. To find issues sooner, many of our bounty programs provide rewards for finding issues prior to products and services reaching production or general availability (GA). One example is our Windows Insider Program. These bounty programs encourage researchers to report vulnerabilities in pre-GA builds to help us get early visibility into any issues.

Our approach to building one of the industry's best bounty programs has drawn top external security researchers to participate, further securing our products and the security community at large.

We've paid out millions of dollars in bounty rewards to hundreds of researchers this year alone, and we're fully committed to investing further in this program. We also recognize researchers who report vulnerabilities even

if they don't qualify for a bounty award under the program to ensure their contributions to customer security are acknowledged.

To ensure that we continue to build a community of security researchers and acknowledge their work, we bring this group together once a year at our BlueHat event. We encourage a deeper engagement between our engineering community, our internal security researchers, and external research community so that we all learn from each other and help protect our communities collectively. We recently wrapped up our October 2023 BlueHat event, with more than 400 researchers joining us from around the world in Redmond, Washington—recordings forthcoming.

Setting the standard for greater transparency

We understand that our customers want the most up-to-date information possible about known issues and potential security vulnerabilities that affect the Microsoft products they use. Communication is critical not only to build and maintain trust with our customers but also to ensure the greater security community has all the information they need to continue defending against the varied attacks threat actors are launching every day.

We're committed to providing detailed communications to our customers regarding security incidents that impact their business. From the MSRC blog to the Security Update Guide, we deliver information to help customers fully address any vulnerabilities in our products and to streamline the security update process. We also notify our customers directly through the message center. But we're not stopping there. These advances in transparency and mitigating cloud vulnerabilities cover just one area in which we are improving the security of our technology. Read about our other engineering advances in EVP of Microsoft Security Charlie Bell's memo to all Microsoft engineers.

The increased speed, scale, and sophistication of cyber threats today and tomorrow demand a new response vulnerability response approach. As part of the Microsoft Secure Future Initiative, we're committed to setting a high standard for the industry as a whole. Through accelerated response times, deeper collaboration, and greater transparency, we are dedicated to building trust with our customers and the community and remaining constantly vigilant.

- **Learn more** about MSRC's mission and the work we do regarding vulnerability discovery and incident response.
- **Learn more** about how Microsoft builds security into everything we design, develop, and deliver.