MONTHLY THREAT BRIEF

April 2026

THIS MONTH IN CYBER

Key Developments shaping operational risk in April 2026

At a Glance

User-Level Exposure Increasing

Patch & Vulnerability Pressure

Collaboration & Social Engineering

Platform-Based Social Engineering Expands

Attackers are increasingly moving beyond traditional phishing into trusted collaboration platforms like Microsoft Teams, impersonating internal IT or helpdesk personnel to initiate contact. By guiding users to launch legitimate remote support tools, they gain direct access while blending into normal business workflows, allowing them to bypass email security controls and operate with reduced visibility.

What To Do

- Require verification for all internal support requests
- Monitor and log remote support tool usage
- Train users to treat unexpected requests with caution

Vulnerability & Exposure Risk Increasing

User-level exposure points like browser extensions are being leveraged to collect sensitive data, highlighting how system-level vulnerabilities and everyday tools are combining to expand overall risk.

What To Do

- Prioritize remediation based on exploitability
- Focus on externally exposed systems first
- Audit browser extensions and remove unnecessary tools

Brief

Helpdesk Impersonation

Threat actors are impersonating IT support through collaboration tools, convincing users to initiate remote sessions and grant access. These interactions often appear legitimate and occur within normal workflows, making them more difficult for users and security controls to identify.

High Volume of Vulnerabilities & Active Exploitation

April saw a surge in disclosed vulnerabilities across major platforms, reinforcing the need for prioritization over volume-based patching.

Browser Extension Data Exposure

Malicious Chrome extensions tied to coordinated campaigns are collecting sensitive user data and credentials. These tools often operate with broad permissions, allowing them to go undetected within user environments.

CONTINUED ON NEXT PAGE »

EMERGING THREAT SURFACE

Identity, Access, and User-Level Risk

Browser & User-Level Data Exposure

User-installed tools such as browser extensions are creating new pathways for data access, often with broad permissions and minimal oversight. These tools can access sensitive information like credentials, session data, and browsing activity, making them a quiet but effective entry point within user environments.

What To Do

- Audit and restrict browser extensions
- Limit permissions for non-essential tools
- Monitor for unusual browser activity
- Enforce allowlists for approved extensions where possible

Living-off-the-Land Attacks Increasing

Attackers are using built-in system tools to carry out activity, blending into normal operations and avoiding detection. By leveraging legitimate administrative utilities, they can execute commands, move laterally, and maintain access without introducing obvious malicious files.

What To Do

- Monitor administrative tool usage
- Establish baselines for normal behavior
- Investigate unusual command execution
- Limit unnecessary administrative privileges

Identity & Trusted Access Abuse

Threat actors are continuing to rely on valid accounts, collaboration tools, and trusted access paths rather than traditional exploitation.

What To Do

- Strengthen identity monitoring and alerting
- Enforce least privilege across accounts
- Monitor for unusual login and session behavior

Helpdesk & Internal Impersonation

Threat actors are leveraging internal communication platforms to impersonate support personnel and bypass traditional phishing detection.

What To Do

- Require verification for internal support requests
- Restrict and monitor remote access tools
- Train users to validate unexpected requests

CONTINUED ON NEXT PAGE »

EMERGING THREAT SURFACE

Infrastructure, Vulnerabilities, and Operational Risk

Endpoint & Security Tool Targeting

Security tools and endpoint platforms are being targeted post-access to escalate privileges and maintain persistence. Once inside an environment, attackers often focus on disabling or bypassing protections to operate with less resistance and extend their access.

What To Do

- Monitor for privilege escalation behavior
- Validate endpoint protection configurations
- Investigate abnormal system-level activity
- Ensure security tools are tamper-protected and properly configured

Critical Infrastructure & Operational Exposure

Threat actors continue targeting infrastructure environments where disruption can extend beyond IT systems. These environments often include operational technology and externally exposed systems, where limited visibility and legacy configurations can increase risk.

What To Do

- Strengthen visibility across IT and OT systems
- Monitor externally exposed infrastructure
- Align cyber response with operational impact
- Regularly assess and secure externally facing assets

Accelerated Exploitation Timelines (AI Impact)

Advancements in AI-assisted techniques are reducing the time between vulnerability discovery and exploitation.

What To Do

- Prioritize patching for critical vulnerabilities
- Reduce exposure windows for external systems
- Test detection and response timelines

Vulnerability Volume & Patch Pressure

A high volume of vulnerabilities, including actively exploited flaws, is increasing pressure on organizations to act quickly and strategically.

What To Do

- Prioritize based on exploitability and exposure
- Focus on internet-facing systems first
- Track known exploited vulnerabilities

CONTINUED ON NEXT PAGE »

STRATEGIC TAKEAWAYS

April 2026

Across this month's developments, several consistent themes are emerging for security and IT teams. Rather than focusing on individual incidents, these signals highlight where organizations should be directing attention as risk continues to evolve.

Social Engineering Is Moving Into Trusted Platforms

Attackers are shifting away from traditional phishing toward collaboration tools and internal communication channels, increasing success rates and reducing user suspicion. Because these interactions occur in platforms users already trust, they are harder to detect and more likely to succeed.

Patch Prioritization Is Becoming Critical

The volume and exploitation of vulnerabilities highlights the need to prioritize remediation based on risk and exposure, not just patch cycles. With more vulnerabilities being exploited quickly after disclosure, organizations must focus on reducing exposure where it matters most.

Everyday Tools Are Expanding the Attack Surface

Browser extensions, remote support tools, and common applications are creating new pathways for data access and persistence. Because these tools are often user-approved and operate within normal workflows, they can introduce risk without triggering traditional security controls.

Resilience Depends on Speed and Coordination

Organizations must prioritize rapid detection, clear escalation paths, and coordinated response across teams to limit impact. The ability to respond quickly and cohesively can significantly reduce operational disruption.

Attack Timelines Continue to Shrink

Faster vulnerability discovery and exploitation are reducing the time organizations have to detect and respond. This leaves less room for delayed action and increases the importance of early detection and continuous monitoring.

CONTINUED ON NEXT PAGE »

THREAT INTELLIGENCE SOURCES

Critical Path Security Advisory: Defending Against Attacks from Compromised Networks

Our latest blog provides guidance on defending against attacks originating from large networks of compromised devices, including recommendations to strengthen network visibility, reduce external exposure, and implement controls.

Read the Full Analysis

Sources & Further Reading

Infrastructure, Policy & Strategy

- Microsoft: Cross-Tenant Helpdesk Impersonation & Data Exfiltration
- CSA Urges CISOs to Prepare for Accelerated AI Threats
- Microsoft April 2026 Patch Tuesday Addresses 160+ Vulnerabilities

Threat Intelligence & Activity

- 108 Malicious Chrome Extensions Caught Stealing User Data
- Microsoft Defender Zero-Day Vulnerability Discovered
- CISA Adds Exploited Vulnerabilities to Known Catalog

Stay Connected

Follow us on social media for the latest updates: