Zero-Days Don't Wait

Neither Can You

LEAPFROG®

Zero-Days Don't Wait — Neither Can You

In today's cybersecurity landscape, zero-day vulnerabilities – flaws in software that are unknown to the vendor and exploited before a fix is available – are no longer rare anomalies. They're routine, relentless, and ruthlessly exploited. And if your business still relies on periodic patching, applying software updates on a regularly scheduled basis instead of in real time, you're already exposed.

In just one week recently, six+ critical zero-days were disclosed across major platforms, including Microsoft, Apple, Fortinet, Ivanti, and others. These weren't theoretical risks. They were actively exploited before patches were released, leaving businesses scrambling to respond.

Zero-Day Exploits Are Accelerating

According to Google's 2024 Zero-Day Trends, 75 zero-day vulnerabilities were exploited in the wild last year, with a sharp increase in attacks targeting enterprise and security products. Nearly half of these flaws were aimed at technologies like firewalls, endpoint protection, and networking appliances – the very tools designed to keep your business safe.

One of the most alarming examples? A critical zero-day in Microsoft SharePoint was weaponized in a large-scale campaign before a patch was even available. Attackers used deserialization flaws to execute remote code, forge trusted payloads, and move laterally across networks, all while blending in with legitimate activity. Over 85 servers were compromised across 29 organizations, including government agencies and multinational firms. (The Hacker News)

And it's not just enterprise platforms. Consumer-grade devices and apps are also under siege. Recent exploits in WhatsApp, FreePBX, and TP-Link routers have been flagged by BleepingComputer and CISA as active threats. These vulnerabilities are often overlooked in SMB environments, especially when employees work remotely, using outdated or unsupported hardware.

Why Periodic Patching Isn't Enough

Attackers are moving faster than ever. By the time your next scheduled update rolls around, the damage may already be done. Today's threat environment demands:

- **Emergency patching capacity:** The ability to deploy fixes immediately, not quarterly.
- **Assume-breach models:** Operating under the assumption that attackers may already be inside.
- **Continuous vulnerability management:** Real-time scanning, prioritization, and remediation.

Executive Call to Action

If your organization still relies on periodic patching, it's time to evolve. Invest in continuous vulnerability management and round-the-clock monitoring with Leapfrog – before attackers find the gap.

At Leapfrog, we have over 25 years of experience helping SMBs leap ahead of threats, not just react to them. Our team stays ahead of the latest zero-day intelligence and brings the operational muscle to protect your business, without the cost of building an internal security department. If you are ready to Leap Ahead of threats to your organization, reach out today to inquire about our Ring of Security CyberRisk assessment.

96%
say they will continue to partner with Leapfrog for the next 12 months

97%
say Leapfrog is more effective than their in-house IT staff

96%
are happy with our after-hours support

97%
have confidence in Leapfrog security

If you're ready to assess your threat level, Leapfrog is ready to help. Please call 866-260-9478 or contact us at sales@leapfrogservices.com.

@leapfrogservices | 404.870.2122 | www.LeapfrogServices.com | 1190 W. Druid Hills Dr. Ste. 200, Atl, GA 30329