NEWS RELEASE

Rapid7 Finds Nearly Two-Thirds of Vulnerabilities Exploited in Q2 2026 Required No User Interaction to Initiate

2026-08-18

Newly exploited vulnerabilities jumped from 8% to 40% in Q2 2026, outpacing traditional patch cycles

BOSTON, Aug. 18, 2026 (GLOBE NEWSWIRE) -- **Rapid7, Inc.** (NASDAQ: RPD), a global leader in AI-powered managed cybersecurity operations, today released its **Quarterly Threat Landscape Report**, revealing that rising vulnerability volumes and faster weaponization are breaking traditional patching models. The findings reinforce that security teams must move beyond static severity scores and prioritize the exposures attackers can realistically exploit.

As AI accelerates flaw discovery, the critical challenge for defenders is no longer just finding bugs - it is acting before adversaries do. According to the report, high and critical disclosures doubled year-over-year to 8,539, with newly exploited vulnerabilities jumping by up to 40%. With the window between disclosure and active exploit collapsing, relying on static CVSS scores and periodic patching is no longer viable.

“Security teams are chasing ghosts if they think they're 'secure' just by closing tickets based on CVSS scores. We're drowning in a deluge of disclosures, and the gap between a patch existing and an exploit being weaponized has collapsed to near zero,” said Christiaan Beek, Vice President, Rapid7 Labs. “If you're still relying on periodic patch cycles while your adversary is automating their kill chain, you aren't managing risk, you're just subsidizing the attackers' R&D. Stop collecting CVEs and start focusing on the exposures that actually matter.”

Key findings include:

- Zero-click vulnerabilities increased. 62% of newly exploited vulnerabilities were “holy grail” flaws that could be exploited over a network without authentication or user interaction.

- Weaponization signals accelerated. The volume of critical vulnerabilities increased 21% quarter over quarter, while publicly available proof-of-concept code rose 12% from the previous quarter and 76% year over year, expanding the pool of vulnerabilities attackers can quickly turn into real-world attacks.
- Missing authentication created a growing attack surface. Disclosures involving missing authentication increased 247% year over year, from 45 to 156.
- Ransomware remained concentrated but continued expanding geographically. The United States accounted for 881 listed ransomware victims, approximately nine times the 99 recorded in Germany. India and Thailand also entered the quarter's top 10 countries, indicating that ransomware affiliate programs are extending beyond their historically prominent U.S. and European targets.

The report also documents state-aligned campaigns from Iran, North Korea, and Russia targeting critical infrastructure and enterprise sectors. Key tactics included exploiting SOHO edge routers for DNS hijacking and actively targeting operational technology and industrial control systems.

What this means for security operations

The second quarter of 2026 makes clear that the traditional wait-and-see patch cycle is no longer enough. With vulnerability disclosures surging and attackers increasingly automating discovery, security teams need to focus less on chasing every new flaw and more on reducing exposure that is actually reachable and exploitable. That shift toward evidence-based exposure management is at the heart of a preemptive security approach.

To read a full copy of the report, visit **here**.

About the Rapid7 Quarterly Threat Landscape Report

The Rapid7 Threat Landscape Report is a quarterly analysis of global adversary behavior drawn from the company's managed detection and response operations, vulnerability intelligence platforms, and threat research telemetry. The Q2 2026 edition examines accelerating vulnerability disclosure and weaponization, geopolitical cyber activity, evolving social engineering tactics, dark web activities, and ransomware trends.

About Rapid7

Rapid7, Inc. (NASDAQ: RPD) is a global leader in AI-powered managed cybersecurity operations, trusted to advance organizations' cyber resilience. Open and extensible, the Rapid7 Command Platform integrates security data, enriching it with AI, threat intelligence, and 25 years of expertise and innovation to reduce risk and disrupt attackers. As a recognized leader in preemptive managed detection and response (MDR), Rapid7 unifies exposure and detection to transform the cybersecurity operations of more than 11,500 customers worldwide. For more information, visit our **website**, check out our **blog**, or follow us on **LinkedIn** or **X**.

Media Contact

Christine Nurnberger
SVP Global Marketing and Growth
press@rapid7.com

Rapid7 Investor Contact
Ryan Flanagan
ICR for Rapid7
investors@rapid7.com
(617) 865-4277

Source: Rapid7