NEWS RELEASE

# Rapid7 Report: Vulnerability Intelligence Shows Significant Year-Over-Year Increase in Widely Exploited Security Flaws

3/28/2022

BOSTON, March 28, 2022 (GLOBE NEWSWIRE) -- **Rapid7, Inc.** (NASDAQ: RPD), a leading provider of security analytics and automation, today announced the release of its latest Vulnerability Intelligence Report examining the 50 most notable security vulnerabilities and high-impact cyberattacks in 2021.

On any given day, security professionals must prioritize and address viable threats from an overwhelming number of reported vulnerabilities. Rapid7 researchers analyze thousands of vulnerabilities each year to understand root causes, dispel misconceptions, and share information on why certain flaws are more likely to be exploited than others. From this research, the team creates a report of the highest priority CVEs based on their likelihood of widespread exploitation.

“We research and publish this report to contextualize the vulnerabilities that introduce serious risk to a wide range of organizations,” said vulnerability research manager and lead Vulnerability Intelligence Report author, Caitlin Condon. “Our goal is to highlight exploitation trends, explore attacker use cases, and offer a framework for understanding new security threats as they arise.”

The **Rapid7 2021 Vulnerability Intelligence Report** highlights 50 vulnerabilities from 2021 that posed considerable risk to businesses of all sizes. Of those 50 vulnerabilities, 43 were exploited in the wild. Furthermore, vulnerabilities classified as “widespread threats” for the scale at which they were exploited increased 136% over the previous year.

Key findings from the research report include:

- Broad, opportunistic exploitation increased significantly in 2021. 66% of vulnerabilities in this report were classified as widespread threats, compared to only 28% in 2020.
- More than 60% of widespread threats cited in this report have been used in ransomware operations, and more than half of widespread threats began with a zero-day exploit.
- More than half (52%) of the known exploited vulnerabilities in this report came under attack within one week of public disclosure, and the average time to known exploitation decreased from 42 days in 2020 to just 12 days in 2021.

“In years past, vulnerabilities and hacking incidents led to fewer widespread attacks,” added Condon. “The recent increase in ransomware, coin mining, and other widespread attacks means the probability of an 'average business' being targeted has correspondingly increased.”

To access the complete Rapid7 2021 Vulnerability Intelligence Report and related resources **click here**.

About Rapid7
Rapid7 (Nasdaq: RPD) is advancing security with visibility, analytics, and automation delivered through our Insight cloud. Our solutions simplify the complex, allowing security teams to work more effectively with IT and development to reduce vulnerabilities, monitor for malicious behavior, investigate and shut down attacks, and automate routine tasks. Over 10,000 customers rely on Rapid7 technology, services, and research to improve security outcomes and securely advance their organizations. For more information, visit our **website**, check out our **blog**, or follow us on **LinkedIn** or **Twitter**.

Press contact:
Kelly Crummey
Corporate Communications
**press@rapid7.com**
(617) 921-8089

Investor Contact:
Sunil Shah
Vice President, Investor Relations
**investors@rapid7.com**
(617) 865-4277

Source: Rapid7