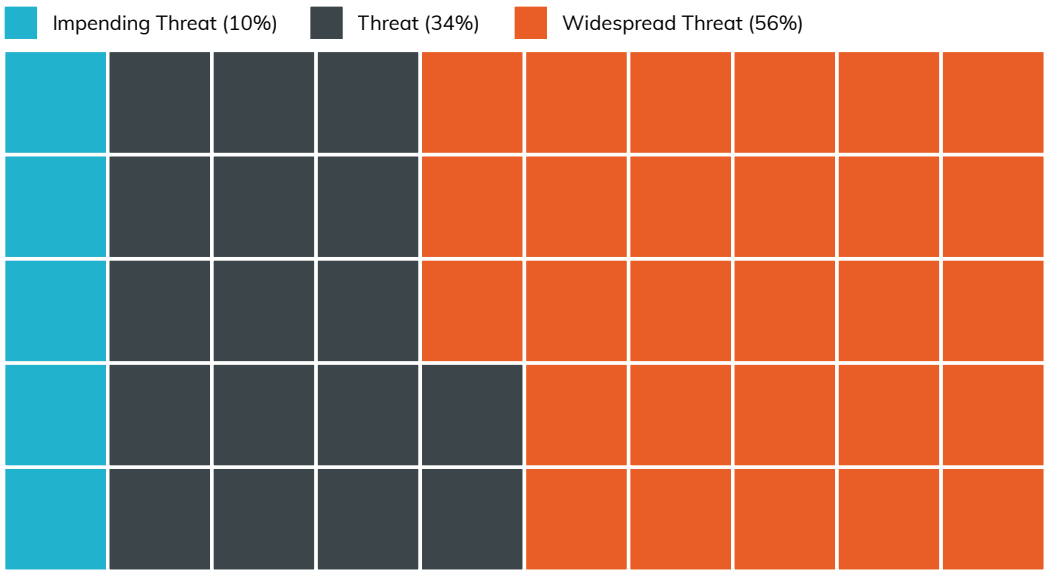
2022 Vulnerability Intelligence Report: Less Bad News, But More Complexity

In some ways, the 2022 attack landscape offered security practitioners a slight respite from the brutal onslaught of mass exploitation and zero-day threats that 2021 left in its wake. Widely exploited vulnerabilities were nominally lower in 2022, though they still comprised the lion's share of CVEs Rapid7 researchers tracked last year. Most "4Shell" fears failed to live up to their namesake, but they nevertheless consumed an inordinate amount of security team time and resources. And while average time to known exploitation fluctuates year over year, a higher percentage of vulnerabilities are being exploited within seven days of public disclosure — an alarming trend.

2022 Vulnerabilities by Threat Status



Exploitation Status Comparison:

Actively exploited

2022

in report were **ACTIVELY** exploited

2021

in report were **ACTIVELY** exploited

Level of Exploitation Comparison:

Widespread

2022

in report are **WIDELY** exploited

2021

in report are **WIDELY** exploited

Time to Exploitation Comparison:

Within 7 days

2022

56%

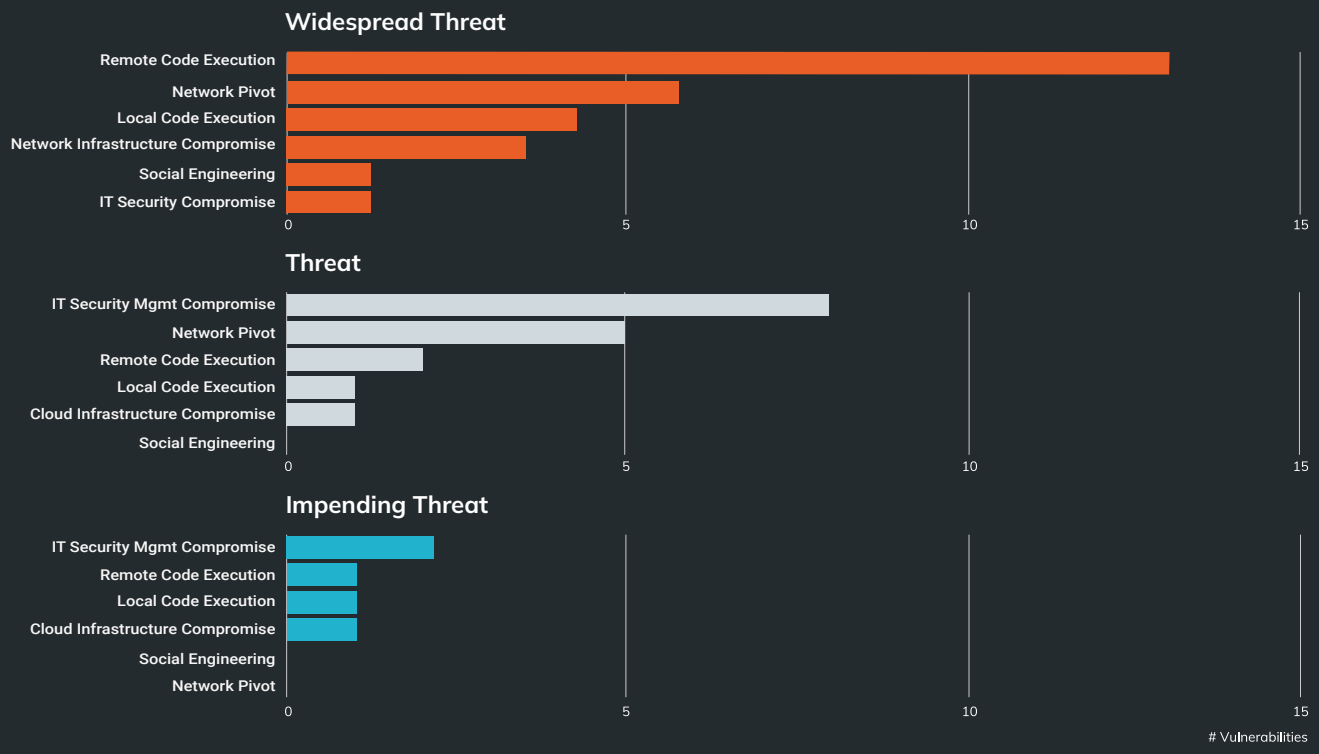
in report were exploited within seven days of public disclosure

2021

50%

in report were exploited within seven days of public disclosure

2022 Vulnerabilities by Attacker Utility and Threat Status



Vulnerability prioritization in 2022 was nuanced, and our analysis emphasizes both the seriousness of long-term exploit trends and the small but real ways attacks relented ever so slightly. As always, solid vulnerability management practices are fundamental to mitigating risk from both novel and known threats and we move through 2023 and beyond.

Get the full Rapid7 2022 Vulnerability Intelligence Report

DOWNLOAD REPORT

RAPID7

PRODUCTS

Cloud Security
XDR & SIEM
Threat Intelligence
Vulnerability Risk Management
Application Security
Orchestration & Automation
Managed Services

CUSTOMER SUPPORT

Call +1.866.380.8113

To learn more or start a free trial, visit: https://www.rapid7.com/try/insight/