



NEWS RELEASE

Cisco's Kenna Security Research Shows the Relative Likelihood of An Organization Being Exploited

2022-01-19

SAN JOSE, Calif., Jan. 19, 2022 /PRNewswire/ --

News Summary:

- A record-breaking 20,130 software vulnerabilities were reported in 2021 – 55 a day on average. However, only 4% of them pose a high risk to organizations.
- An organization can greatly reduce its chance of breach, or "exploitability score," by up to 29 times by first fixing high-risk vulnerabilities with public exploit code and having a high remediation capacity.
- Using Twitter mentions to prioritize software fixes is twice as effective at reducing exploitation as the industry-standard Common Vulnerability Scoring System (CVSS).

A record-breaking 20,130 vulnerabilities were reported in 2021. However, only 4% pose a high risk to organizations.

New research has quantified the success of various strategies for vulnerability management and the exploitability of entire organizations, expanding the risk-based playbook for cybersecurity practices.

With an [average of 55](#) new software vulnerabilities published every day in 2021, even the best staffed and resourced IT teams cannot fix all of the vulnerabilities across their infrastructures. Fortunately, there is a better solution.

The research conducted by [Kenna Security](#), now part of Cisco and a market-leader in risk-based vulnerability management, and the [Cyentia Institute](#), shows that properly prioritizing vulnerabilities to fix is more effective than increasing an organizations' capacity to patch them, but having both can achieve a 29 times reduction in an organizations' measured exploitability.

The findings are explained in Kenna's latest report, [Prioritization to Prediction, Volume 8: Measuring and Minimizing Exploitability](#).

"Exploitations in the wild used to be the best indicator for which vulnerabilities security teams should prioritize. Now we can show the likelihood of a particular organization being exploited, which is what we've always wanted to do," said Ed Bellis, co-founder and chief technology officer of Kenna Security, now part of Cisco. "This gives organizations a much better chance at combating potential cyber threats effectively and the research shows that our customers are successfully managing their vulnerability risk every day."

Exploitability was determined using the open Exploit Prediction Scoring System (EPSS); a cross-industry effort including Kenna Security and the Cyentia Institute that is maintained by FIRST.org.

The research confirms a [recent Cybersecurity and Infrastructure Security Agency \(CISA\) directive](#) that suggests it's wiser to move away from prioritizing fixing of vulnerabilities based on CVSS scores and instead focus on high-risk vulnerabilities. Analysis shows that factors like exploit code and even Twitter mentions are better signals than CVSS scores.

"It's clear that a shift to exploitability is going to make a huge difference based on the data and findings in this report. An analysis of CISA's published vulnerabilities suggests that they may also be moving course away from CVSS scores as we were conducting this research," said Wade Baker, partner and co-founder of Cyentia Institute. "We took it a step further to account for remediation velocity when making our calculations, which should better inform security teams."

The research also suggests that:

- Nearly all (95%) IT assets have at least one highly exploitable vulnerability.
- Prioritizing vulnerabilities with exploit code is 11 times more effective than CVSS in minimizing exploitability.
- Most (87%) organizations have open vulnerabilities in at least a quarter of their active assets, and 41% of them show vulnerabilities in three of every four assets.
- A strong 62% majority of vulnerabilities have less than a 1% chance of exploitation. Only 5% of CVEs exceed 10% probability.

Additional Resources

- Read the full report, "[Prioritization to Prediction, Volume 8: Measuring and Minimizing Exploitability](#)," the latest installment of Kenna Security's [series](#)
- Read the [blog](#)
- Engage with Kenna on [Twitter](#), [Facebook](#), and [LinkedIn](#).

About Cisco

Cisco (NASDAQ: CSCO) is the worldwide leader in technology that powers the Internet. Cisco inspires new possibilities by reimagining your applications, securing your data, transforming your infrastructure, and empowering your teams for a global and inclusive future. Discover more on The Network and follow us on Twitter.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.

View original content to download multimedia: <https://www.prnewswire.com/news-releases/ciscos->

[kenna-security-research-shows-the-relative-likelihood-of-an-organization-being-exploited-301463427.html](https://www.cisco.com/c/en/us/solutions/cyber-excelerate/whitepapers/kenna-security-research-shows-the-relative-likelihood-of-an-organization-being-exploited-301463427.html)

SOURCE Cisco Systems, Inc.