Cyber Liability

CISA's Known Exploited Vulnerability Catalog Explained

The Cybersecurity & Infrastructure Security Agency (CISA) maintains the Known Exploited Vulnerability (KEV) catalog to help organizations better manage and mitigate cybersecurity vulnerabilities. The agency encourages organizations to utilize the KEV catalog—the authoritative list of vulnerabilities that have been exploited—to keep pace with threat activity and remediate the listed vulnerabilities to reduce the likelihood of compromise by known threat actors. The list of vulnerabilities is updated on a regular basis and identifies top risks that organizations should address immediately.

While only federal civilian executive branch (FCEB) agencies are required to remediate vulnerabilities identified in the KEV catalog, CISA strongly recommends all organizations include a requirement to address KEV catalog vulnerabilities to build collective resilience across the cybersecurity community. The KEV catalog requires all FCEB agencies to remediate issues within a specified timeframe. These strict remediation timelines should be a consideration for agencies and enterprises intending to use the KEV catalog.

Overall, the KEV catalog can help organizations prioritize their cybersecurity remediation efforts based on adversary activity. It can also give organizations the opportunity to manually fill in gaps that vulnerability scanners or automated vulnerability solutions may not detect.

For more risk management guidance, contact us today.