Bugcrowd Reports 185% Increase in High-Risk Vulnerabilities within Financial Sector

Submitted by: Bugcrowd
Tuesday, 18 January 2022

2022 Priority One Report Cites Increasing Need for Crowdsourced Security Due to Rapid Digital Transformation

SAN FRANCISCO, CA – January 18, 2022 – Bugcrowd, the leader in crowdsourced cybersecurity, today released its 2022 Priority One report to spotlight the key cybersecurity trends of the past year, including the rise in the adoption of crowdsourced security due to the global shift to hybrid and remote work models, and the rapid digital transformation associated with it. The report reveals that the strategic focus for many organisations across industries has shifted, with the emphasis now on clearing residual security debt associated with that transformation. In particular, financial services companies on Bugcrowd's platform experienced a 185% increase in the last 12 months for Priority One (P1) submissions, which refer to the most critical vulnerabilities.

According to activity recorded on the Bugcrowd Security Knowledge Platform™, high-level trends included an increase in ransomware and the reimagining of supply chains, leading to more complex attack surfaces during the pandemic. Ransomware overtook personal data breaches as the threat that dominated cybersecurity news across the world in 2021. Global lockdowns and remote work caused a rush to put more assets online, which led to an increase in vulnerabilities. In turn, security buyers invested heavily to incentivise ethical hackers to find critical threats, causing P1 and P2 bugs to make up 24% of all valid submissions for the year.

In the past, Advanced Persistent Threats (APTs) were defined by highly advanced tactics and clandestine operations, but this approach started to shift in 2021 toward more commonplace tactics such as so-called N-day exploits, which are attacks on known vulnerabilities. Diplomatic norms around hacking have weakened to the point where nation-state attackers are now less concerned with being stealthy than in the past.

"Significantly, we've seen a democratisation of such threats due to an emerging ransomware economy and a continued blurring of lines between state actors and e-Crime organisations," said Casey Ellis, Founder and Chief Technology Officer for Bugcrowd. "All of which, combined with growing and more lucrative attack surfaces, have made for a highly combustible environment. In 2022, we expect more of the same."

Some top highlights from the 2022 Priority One Report include:

• Cross Site Scripting was the most commonly identified Vulnerability Type
• Sensitive Data Exposure moved up to #3 from #9 on the list of Top 10 most commonly identified Vulnerability Types
• Ransomware went mainstream, and governments responded
• Supply chains became a primary attack surface
• Penetration testing entered a renaissance

Security Industry Trends from 2021

2021 was the year Vulnerability Disclosure became a major concern for government agencies in particular. Total valid submissions in the Government sector were up an astonishing 1,000% for the year. Most submissions occurred in the third quarter, as government buyers invested in crowdsourced security in response to new federal civilian agency directives that made Vulnerability Disclosure a key requirement.

In the Financial Services and Software sectors, the report documents increased levels of ethical hacker activity as a function of making up for a long tail of security debt. It also shows increased severity levels and higher payouts to incentivise the discoveries made by security researchers.

Accelerated digital transformations increased efforts to strengthen security postures, as a greater share of revenue came from online transactions. Financial services companies had to move quickly on this issue due to the sector's critical importance for businesses and consumers. Valid submissions were up 82% across the FinServ sector. In addition, researcher payouts for discoveries grew 106% in FinServ. In the Software sector – a bellwether for the cybersecurity ecosystem as a whole – total researcher payouts were up by 73%, reflecting the increasingly impactful nature of validated bugs.

Click here to download a copy of the full report.

About Bugcrowd

Bugcrowd is the leading provider of crowdsourced cybersecurity solutions purpose-built to secure the digitally connected world. Today's enterprise demands an offensive approach to cybersecurity—and Bugcrowd offers the only solution that orchestrates data, technology, and human intelligence to expose blind spots. The Bugcrowd Security Knowledge Platform™ enables businesses to do everything proactively possible to protect their organisation, reputation and customers with products like Bug Bounty, Penetration Testing-as-a-Service, and more. Trusted by organisations across the globe, Bugcrowd uncovers and remediates vulnerabilities before they interrupt business by leveraging expert ingenuity and the knowledge of world-class security researchers. Based in San Francisco, Bugcrowd is backed by Blackbird Ventures, Costanoa Ventures, Industry Ventures, Paladin Capital Group, Rally Ventures, Salesforce Ventures and Triangle Peak Partners. Learn more at www.bugcrowd.com.

Contacts:

Rose Ross for Bugcrowd EMEA
Omarketing
rose@omarketing.com
+44 (0)7976 154 597