Intigriti launches fast lane program to incentivise cybersecurity research

BY INTIGRITI · AUGUST 10, 2021 · LAST UPDATED ON MARCH 6, 2025

Today, we are launching the first 'fast lane' program that enables security researchers to monetize novel cybersecurity research prior to public disclosure. The initiative aims to effectively connect finders of emerging threats with affected organisations, allowing them to prepare and respond in a timely manner. This allows researchers to collect monetary 'bug bounties' for all participating companies, maximising their return on investment before releasing their work to the public.

"*Every year, one way or another, someone manages to break the internet by discovering a groundbreaking new attack vector that affects thousands of companies*," says Inti De Ceukelaire, Head of Hackers at Intigriti. "*Unlike so-called zero-days, these techniques do not rely on a single vulnerability in popular software. Instead, they involve vulnerable patterns, configuration and implementation mistakes that may be much harder to detect and mitigate. For that reason, Intigriti allows qualifying researchers to tap into their network of private bug bounty programs consisting of more than 300 companies globally that would otherwise be unaccessible for these researchers. In contrast to earlier initiatives by other vendors, 100% of the collected bug bounties go directly to the researcher, and the research remains their intellectual property*".

The idea of assigning priority passes to researchers emerged after an influx of bug bounty reports related to newly uncovered hacking techniques at the hacker conference DEF CON last week: "*We are delighted to see that our community detects these issues merely hours after the research has been published*," De Ceukelaire says, also adding that, "*giving potentially affected companies a heads-up prior to publication reduces their risk of being targeted by malicious actors. Researchers on the other hand receive a dedicated time window to claim their well-deserved bounties.*".

James Kettle, Director of Research at PortSwigger and composer of their yearly top 10 web hacking techniques list affirms that bug bounty can be a facilitator for research, albeit with some caveats:

"*Bug bounty programs enable researchers to explore novel techniques on real systems, and get rewarded for doing so. However, the prevalence of private programs means that people who focus on novel issues can sometimes miss out on the bulk of bounties from their own techniques. Frankly, if my only goal was to maximise my bug-bounty income, I wouldn't spend much time on research. I'm cautiously excited to see Intigriti talking about addressing this, and hopefully making novel research more financially tempting. If this is tackled alongside other barriers to automation-augmented research I think we could see a change of pace in web security research.*"

Intigriti security researcher Alex Birsan, who shook the cybersecurity industry earlier this year with his newly found "dependency confusion" supply chain hacking technique agrees:

"*Before publishing my blog post about dependency confusion, I tried to make sure that as many affected companies as possible were aware of the issue and had a chance to fix it. One of the main obstacles I encountered is that I was unable to report it to some affected vendors because they ran private vulnerability disclosure programs that I did not have access to. If you find a novel and widespread*

security issue, you should always get a chance to let everyone know about it and collect your rightful rewards, regardless of your status in the bug bounty world or other factors. This initiative by intigriti is a significant step in the right direction."

Research can be submitted through Intigriti's fast lane form.

About Intigriti

Intigriti is a pioneering cyber-security company that channels its community of ethical hackers to test their clients' websites and applications for vulnerabilities. Intigriti works with over 300 clients across a wide array of sectors, from small tech start-ups to large banks and airlines. The team works together with Europe's largest ethical hacking community. Their strong focus lies on innovation and outstanding customer service.

REQUEST A DEMO	VISIT THE WEBSITE	GET IN TOUCH
intigriti.com/demo	**intigriti.com**	**hello@intigriti.com**