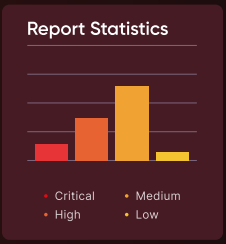
YesWeHack

# VULNERABILITY DISCLOSURE POLICY

A secure and streamlined channel for reporting vulnerabilities that impact your organisation




8
Total Reports

3
Resolved reports

New Reports

#YWH-PGM4922-7
**Server misconfiguration**
Priority P4 CVSS L-3.7

#YWH-PGM4922-2
**Default accounts still valid**
Priority P2 CVSS M-6.5

#YWH-PGM4922-3
**Information disclosure in PDF metadata**
Priority P3 CVSS M-4

## ENABLE RESEARCHERS TO REPORT ANY VULNERABILITIES THEY FIND

With attack surfaces continuing to grow, organisations should help good-faith researchers notify them of any potential vulnerabilities they find in their digital assets. It's up to IT teams to provide a secure, straightforward mechanism to facilitate this process.

YesWeHack provides a simple, secure, technical, and legal framework for reporting potential vulnerabilities in your internet-facing assets - after which you can quickly take the appropriate action.

**A Vulnerability Disclosure Policy, or VDP, is advocated by regulatory agencies such as NIST, ENISA and CISA and prescribed through standards ISO 29147 and ISO 30111.**

### LEARN ABOUT VULNERABILITIES BEFORE BAD GUYS DO

### SHOW YOU'RE SERIOUS ABOUT SECURITY

### STREAMLINE COMMUNICATION AND ELIMINATE 'NOISE'

## PRODUCT FEATURES

- BRANDED, CUSTOMISABLE TEMPLATE
- END-TO-END ENCRYPTED CHANNEL
- IN-HOUSE TRIAGE SERVICE
- UNIFIED VULNERABILITY MANAGEMENT

# VDP VS. BUG BOUNTY

| | VULNERABILITY DISCLOSURE POLICY | BUG BOUNTY |
|---|---|---|
| **WHAT?** | A secure, public, passive mechanism for anyone to legally report vulnerabilities in an organisation's internet-facing assets. | A proactive invitation of ethical hackers (hunters) to probe specific digital assets (scopes), incentivised with financial rewards (bounties) for specific (qualifying) vulnerabilities. |
| **WHY?** | To enable any good-faith researchers to report potential vulnerabilities in any exposed digital assets before malicious actors find them. | To extend security testing capabilities and secure more assets, more rapidly and more comprehensively than with alternative methods. |
| **HOW?** | By providing clear instructions for responsibly reporting vulnerabilities and a secure channel for transmitting all relevant details. | By detailing program rules, in/out-of-scope assets, qualifying bugs, a rewards grid and any relevant testing requirements. |
| **WHO?** | Anyone at all – from security pros flagging technical vulnerabilities to customers who notice sensitive information visible on a public web page. | Only registered and vetted ethical hackers. Private programs are restricted to handpicked, invited hunters. |
| **REWARD?** | No. There should be no incentive or expectation of financial rewards for reporting vulnerabilities. | Yes. The rewards grid is established before launch and is clearly communicated to invited hunters in the program rules. |

**"HAVING A VULNERABILITY DISCLOSURE PROGRAM HAS PROVIDED US WITH A CRUCIAL AND HIGHLY EFFECTIVE CHANNEL FOR COMMUNICATION WITH THE EXTERNAL WORLD."**

Cybersecurity Engineer At Europe's Leading Consumer Electronics Retailer

"Our VDP is mainly used for the brand's image: with this tool in place, it shows that security is taken seriously by the company."

**Deputy CISO Of A Global Luxury Brand**

"We have seen an increasing number of our clients wanting to ensure we have the right processes in place and asking us whether we have a VDP or a Bug Bounty Program."

**Jean Yves Le Breton**, Product Security Manager

GfK

YesWeHack complies with strict security, financial traceability and privacy requirements. YesWeHack's services are ISO 27001- and ISO 27017-certified and accredited by CREST. YesWeHack's infrastructure uses EU-based, GDPR-compliant private hosting that meets the most stringent standards: ISO 27001, ISO 27017, ISO 27018, ISO 27701 and SOC II Type 2. The YesWeHack platform is also permanently subject to a public Bug Bounty Program.