# When A Hacker Comes Knocking

## Vulnerability disclosure, bug bounties, and PCI DSS v4.0

Harley Geiger, Venable LLP

Ilona Cohen, HackerOne

# Who we are

## Harley Geiger

Counsel

Venable LLP

## Ilona Cohen

Chief Legal and Policy Officer

HackerOne

HPC

HACKING POLICY COUNCIL

PCI Security Standards Council

# Overview

1. Hackers vs. Cybercriminals
2. Vulnerability Disclosure Policies (VDPs)
3. Bug Bounties
4. PCI DSS v4.0

# Hackers vs. Cybercriminals

A scientific review

**Hackers:**

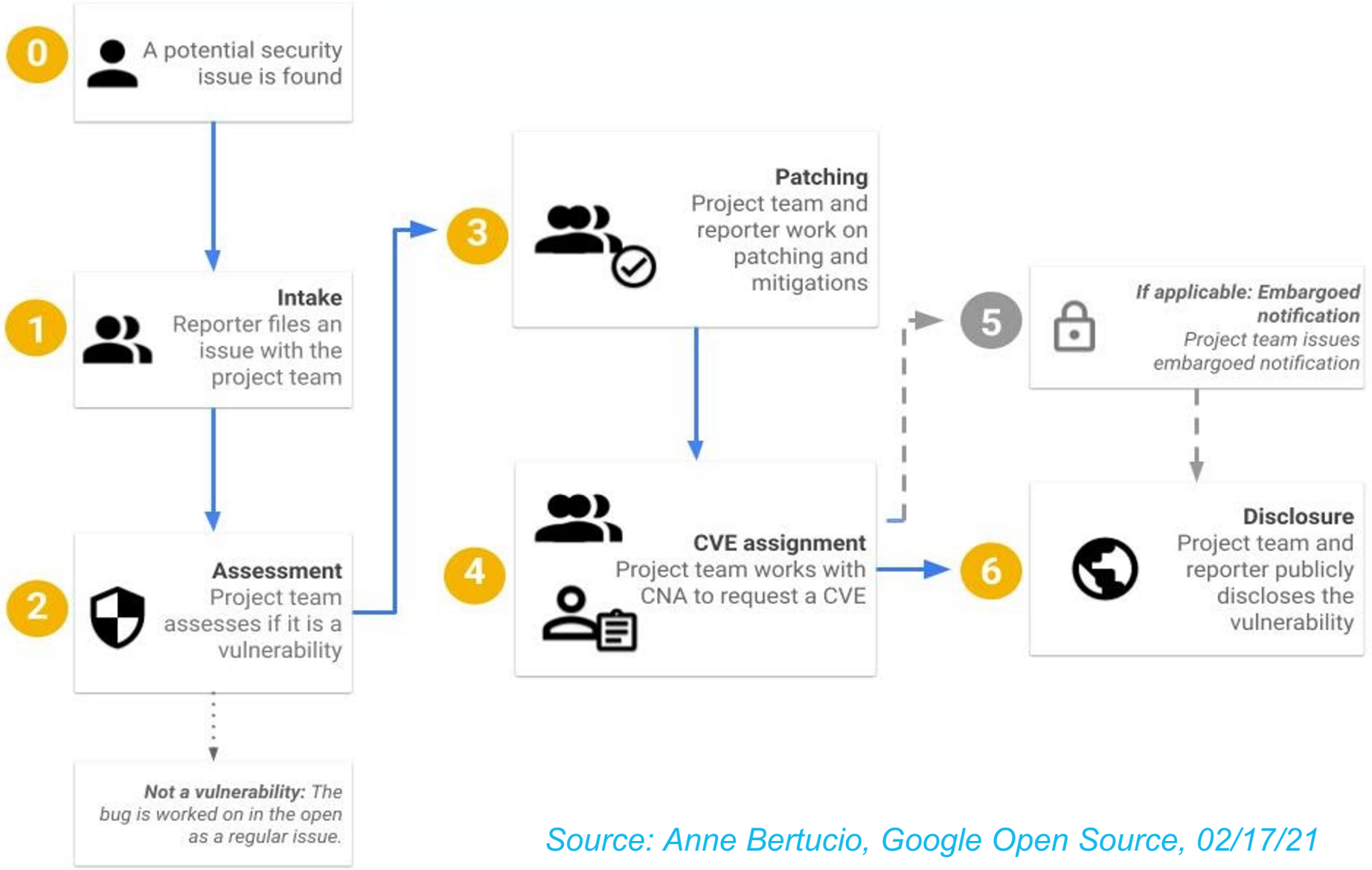
- Wear black hoodies
- Think they're really cool
- May hack without permission
- Hack for the purpose of strengthening the security of products, enterprises, users
- Don't demand money in exchange for disclosing or withholding vulnerabilities
- Don't cause excess damage or data exfiltration
- More likely to use designated disclosure channels

**Cybercriminals:**

- Wear black hoodies
- Think they're really cool
- Hack without permission
- Hack for money, politics, or lulz
- Often make threats and demand money
- May cause damage or data exfiltration
- Less likely to use designated disclosure channels

PCI Security Standards Council

# Vulnerability Disclosure Policies (VDPs)




*Source: Anne Bertucio, Google Open Source, 02/17/21*

# Tips to Ensure VDP Success

- Don’t leave your vuln disclosure channel unattended
- Establish vulnerability management processes to deal with disclosures
- Loop in the legal, compliance, and comms teams
- Communicate with vulnerability reporters about the timeline for mitigation and public disclosure

PCI Security Standards Council

# VDP Examples

## U.S. Department of Defense

Since 2016, the mission of the DoD VDP is to function as the single focal point for receiving vulnerability reports and interacting with crowd-sourced cybersecurity researchers supporting DoD networks. As of May 2023, the program has received 46,786 vulnerabilities reported by 4,860 participating researchers.

## Zebra Technologies

Zebra has maintained a VDP since May 2021, and has resolved nearly 100 vulnerabilities reported by about 100 participating hackers. Zebra's public VDP is a central part of what has become a multi-pronged approach to engaging with hackers, which now includes regular hacker-powered pentests and a private bug bounty program.

## Government Technology Agency of Singapore (GovTech)

Since its launch in 2019, the GovTech VDP has resolved 1,060 reports submitted by 321 participating hackers.

# Hackers Like Rewards; Cybercriminals Extort

“So is this vuln eligible for a reward?”

**vs.**

“Pay me or I’ll publicly disclose your vulns.”

“I’d like to present about this at DEF CON.”

**vs.**

“My DEF CON presentation will include your attempts to silence me.”

PCI Security Standards Council

# VDPs vs. Bug Bounties

Neither involve actual insects.

**Vulnerability disclosure policy:**

- Fundamental security practice
- No payment for vulnerabilities
- Often no authorization to test for vulnerabilities
- Broader scope of assets to test
- Receipt of disclosures on an ongoing basis

**Bug bounty:**

- More disclosures, more maturity required
- Payment provided for vulnerabilities
- Authorization provided for vulnerability testing
- Specific scope of assets that may be tested
- Active identification of vulnerabilities for a set period

PCI Security Standards Council

# Bug Bounty Examples

## PayPal

Since 2018, PayPal's bug bounty program has paid nearly $10M in bounties on more than 1,600 reports submitted by almost 800 participating hackers.

## Starbucks

Starbucks launched its bug bounty program in November 2016, and has since paid over $930k in bounties on more than 1,600 reports submitted by 1,200+ hackers.

## General Services Administration

The General Services Administration (GSA) runs a persistent bug bounty program that rotates services into scope at regular intervals. To date, the program has paid over $65k in bounties on 178 reports. Over 218 hackers have submitted valid reports, some not eligible for bounty payment.

# PCI DSS v4.0

| Requirements and Testing Procedures | Guidance |
| --- | --- |
| **A1.1** Multi-tenant service providers protect and separate all customer environments and data. | |
| **Defined Approach Requirements**<br><br>**A1.2.3** Processes or mechanisms are implemented for reporting and addressing suspected or confirmed security incidents and vulnerabilities, including:<br>• Customers can securely report security incidents and vulnerabilities to the provider.<br>• The provider addresses and remediates suspected or confirmed security incidents and vulnerabilities according to Requirement 6.3.1.<br><br>**Customized Approach Objective**<br><br>Suspected or confirmed security incidents or vulnerabilities are discovered and addressed. Customers are informed where appropriate. | **Purpose**<br><br>Security vulnerabilities in the provided services can impact the security of all the service provider's customers and therefore must be managed in accordance with the service provider's established processes, with priority given to resolving vulnerabilities that have the highest probability of compromise.<br><br>Customers are likely to notice vulnerabilities and security misconfigurations while using the service.<br><br>Implementing secure methods for customers to report security incidents and vulnerabilities encourages customers to report potential issues and enable the provider to quickly learn about and address potential issues within their environment. |

PCI Security Standards Council

# PCI DSS v4.0

| Requirements and Testing Procedures | Guidance |
| --- | --- |
| **6.3** Security vulnerabilities are identified and addressed. | |
| **Defined Approach Requirements**<br><br>**6.3.1** Security vulnerabilities are identified and managed as follows:<br>• New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs).<br>• Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact.<br>• Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment.<br>• Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered. | For control over in-house developed software, the organization may receive such information from external sources. The organization can consider using a "bug bounty" program where it posts information (for example, on its website) so third parties can contact the organization with vulnerability information. External sources may include independent investigators or companies that report to the organization about identified vulnerabilities and may include sources such as the Common Vulnerability Scoring System (CVSS) or the OWASP Risk Rating Methodology. |

PCI Security Standards Council

# PCI DSS Post-Disclosure Obligations

**6.3.3** - Known vulnerabilities in system components must be patched

- Critical – one month
- Non-critical – determined by entity (ex. three months)

**12.10.1** - Activate incident response plan, including legal review of reporting requirements

- Was the CDE compromised?
- Was PII accessed or exfiltrated?
- Were operations or services disrupted?

PCI Security Standards Council

# Takeaways

1. When a hacker comes knocking, it may be to help, not to attack

2. Vuln disclosure policies streamline receipt of vulns from hackers

3. Bug bounties enable orgs to work with hackers to proactively identify vulns

4. VDPs and bug bounties can help orgs comply with some PCI DSS v4.0 requirements

# Resources

- The CERT Guide to Coordinated Vulnerability Disclosure

  *Householder et al., CMU Software Engineering Institute, 2017*

  *https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=503330*

- Beginner's Guide to Bug Bounty Programs

  *HackerOne, https://www.hackerone.com/beginners-guide-bug-bounty-programs*

- Coordinated Vulnerability Disclosure Policies in the EU

  *ENISA, 2022, https://www.enisa.europa.eu/publications/coordinated-vulnerability-disclosure-policies-in-the-eu*

# Thank you!

Harley Geiger, Venable LLP

Ilona Cohen, HackerOne

HACKING POLICY COUNCIL