Setting up a Coordinated Vulnerability Disclosure (CVD) Programme

GSMA Security

October 2020

Table of Contents

What is CVD **1**

Benefits **2**

Key Enablers **2**

FAQ **4**

Best Practice **5**

What is CVD

Coordinated Vulnerability Disclosure

Coordinated Vulnerability Disclosure (CVD) of security vulnerabilities is a well-established process to share knowledge and resolve vulnerabilities. This process allows people or groups, such as security researchers, to report details of security vulnerabilities in products and services, benefiting the company concerned while still protecting their own interests as researchers. CVD, which ought to be a standard component of a security programme, is a framework that sets clear expectations for constructive engagement by all parties to remediate or mitigate the vulnerability.

The early disclosure of vulnerabilities helps to protect end users, allowing vendors and providers of products and services to address security issues before public disclosures are made. A successful CVD programme relies on a clearly defined scope, objectives and legally complete policies which are supported by internal processes.

GSMA Support

The GSMA would like to encourage the mobile ecosystem players, including mobile operators and suppliers to develop their own CVD programmes to promote fixes and mitigating actions to protect customers' security and trust in the mobile communications industry.

This document is designed to help members introduce, understand and evaluate the use of a CVD within their organisations as well as point to best practice. It is important to note that every CVD programme will be different as it will need to be tailored to the local regulation requirements, specific threat profile, and assets of your own organisation.

Benefits

The following outline the benefits of setting up a CVD Programme:

Demonstrates Security Maturity
Having a CVD programme demonstrates a willingness to receive vulnerability reports and creates a culture of trust, transparency and responsibility between organisations and the research world. It also demonstrates a company's commitment to protecting its assets and responding to known vulnerabilities.

Proactive Security Initiative
By setting up a CVD programme you have access to limitless security researchers and organisations with a willingness to continually test your networks and systems. You will receive reports of vulnerabilities and with a structure like CVD, it allows you time to fully consider and mitigate reported issues.

Provides your organisation with time to fix an issue
CVD is a valuable tool that will assist in avoiding legal, brand and reputational damage by providing your organisation with sufficient time to fix the issue and to minimize loss or damage through the formalisation of feedback of a reported vulnerability. It also allows for detailed reporting, time to reproduce and evaluate the issue, and potentially to also work through a solution with the researcher.

Fosters a positive relationship and builds trust with researchers
Researchers are likely to write about your company in more positive, less critical terms if they can see that you want to learn about vulnerabilities and fix them. A properly resourced and managed CVD programme provides a safe environment for researchers to investigate and report vulnerabilities.

Ensures Regulatory Compliance
Increasingly, regulators and other national authorities are mandating that ICT companies establish and run CVD programmes to ensure a mechanism exists to receive and address discovered vulnerabilities. The proactive launch of a CVD programme could preempt the need for regulation.

Key Enablers

Organisations have some flexibility when planning and designing their CVD programmes and they should ensure their programmes can meet the needs of the security research

community, their customers, their security objectives, their risk profile, etc. It is essential that whatever programme is arrived at is clearly documented and adhered to and the critical elements and enablers for any CVD programme include the following:

- A clearly written CVD policy that sets out the ground rules for reporting and managing vulnerabilities
- Dedicated web page that describes the CVD programme and on which the policy can be accessed
- A standardised reporting mechanism for researchers to use e.g. an online form and a dedicated email address
- Documented processes to be followed internally when receiving, reviewing and responding to disclosures received, all in a timely manner
- Sufficient resources to support the programme by undertaking vulnerability analysis and stakeholder communications to ensure researchers are kept up to date and fully informed
- A way to publicly acknowledge researchers and their work such as a hall of fame or a web page

For a more detailed guidance see the Best Practice section at the end of this document.

FAQ

1. What is the cost of setting up a CVD Programme?

Operating a CVD programme is mainly about clear communication channels, clear policy and robust and responsive process, none of which need be inherently expensive. Fixing vulnerabilities may cost money, but this is something you need to do anyway (and a CVD programme will give you more time to do it). Bug bounties require a budget, but these are optional – see the next question.

2. Do I need to provide a bounty for the vulnerability?

Offering a bug bounty can incentivise researchers to look at your products and services. But it is not a requirement, and many researchers will be happy to engage without one.

3. Do I need a Hall of Fame?

A CVD Hall of Fame facilitates the nomination and recognition of other finders that may have made significant discoveries of vulnerabilities to your organization, and acts as an incentive to researchers. The GSMA have their own example of the Industry Mobile Security Hall of Fame which can be found here. Again, though, it is not a requirement, and it is up to each individual organisation to determine whether this is the right approach for them.

Best Practice

The GSMA has identified some best practice documents which will assist you in setting up your own CVD programme.

- CERT guide to CVD https://resources.sei.cmu.edu/asset_files/SpecialReport/2017_003_001_503340.pdf
- ISO https://www.iso.org/standard/72311.html
- Open Source Vulnerability Disclosure Framework https://github.com/bugcrowd/disclosure-policy
- IoT Security Foundation https://www.iotsecurityfoundation.org/wp-content/uploads/2017/01/Vulnerability-Disclosure.pdf
- Netherlands NCSC https://www.enisa.europa.eu/news/member-states/WEB_115207_BrochureNCSC_EN_A4.pdf
- ENISA https://www.enisa.europa.eu/publications/vulnerability-disclosure
- FIRST https://www.first.org/global/sigs/vulnerability-coordination/multiparty/FIRST-Multiparty-Vulnerability-Coordination-v1.0.pdf
- UK NCSC https://www.ncsc.gov.uk/information/vulnerability-disclosure-toolkit

The GSMA CVD programme document FS.23 is also useful for organisations wishing to understand how to better engage with researchers and can be found here.

- FS.23 GSMA CVD Programme

GSMA HEAD OFFICE
Floor 2
The Walbrook Building
25 Walbrook
London
EC4N 8AF
United Kingdom
www.gsma.com