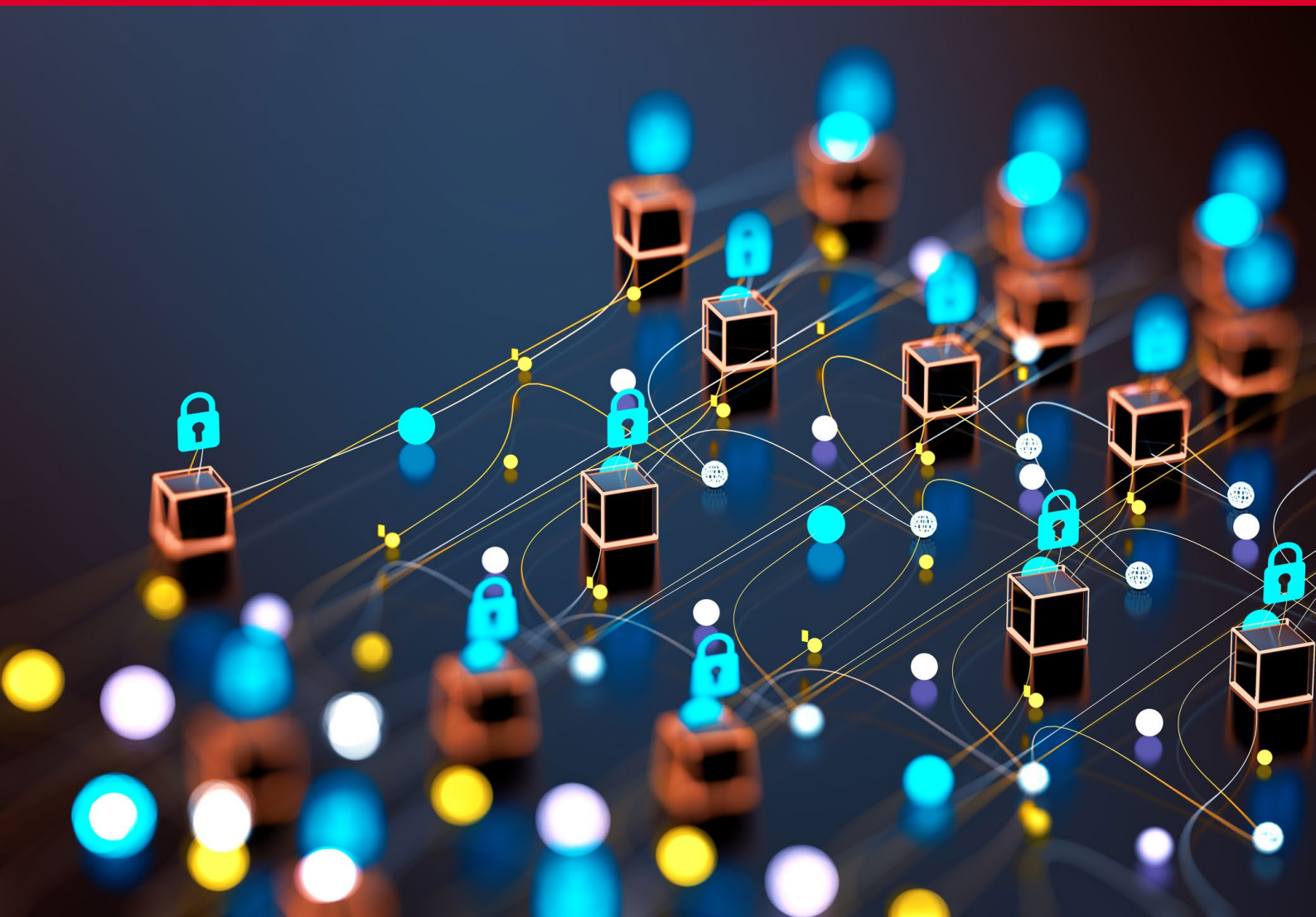
GSMA

May 2024

GSMA Coordinated Vulnerability Disclosure



Contents

An introduction to the CVD Programme

The GSMA regards the security of mobile network infrastructure, and customer equipment such as devices, as essential to the provision of secure and trustworthy services by its Members.

The GSMA Coordinated Vulnerability Disclosure (CVD) Programme gives **security researchers** a route to disclose a vulnerability impacting the mobile ecosystem, meaning the impact can be mitigated before it enters the public domain. We work with mobile operators, suppliers and standards bodies to develop fixes and mitigating actions to protect customers' security and trust in the mobile communications industry.

The GSMA encourages disclosure of security research which enhances security levels and better protects assets and customers, and our CVD Programme is designed to support the reporting and remediation of security vulnerabilities at industry level. We invite both private individuals and organisations to report vulnerabilities to the GSMA in a responsible manner in line with our programme scope.

You can find out more about submitting a vulnerability to the Programme **here**.

Impact of the GSMA CVD Programme

Since our CVD Programme started in 2017 we have considered over 95 vulnerability disclosures, many encapsulating multiple linked vulnerabilities.

The technologies have included:

The GSMA CVD Programme has allowed the industry to improve security in a number of ways thanks to researchers bringing their research on vulnerabilities to the Programme prior to public release.

Recent examples include:

- Removal of weak GPRS encryption algorithms from devices and adding respective device test-cases for new devices, prior to the public release of research identifying the weakness. Update of 3GPP specifications within a week of the release of the research which usually takes several months (see **research**)
- Mandatory inclusion of full-rate user-plane integrity protection for 5G from 3GPP Rel-16, providing protection for an estimated 395 million additional 5G devices (see **research**)
- Issuing of patches to prevent keystream reuse by network equipment that did not follow the standards, prior to public presentation of the research. Also included a new SCAS test for this behaviour during NESAS audits (see **research**)
- Informing MNOs about the exploitation of SIM cards with a vulnerable applet installed and issue guidance to prevent misuse (see **research**)

Where appropriate, CVD submissions and countermeasures are also added to the relevant **GSMA reference document**.

GSMA CVD Programme – disclaimer

The GSMA's responsibilities and any other activities carried out as part of the GSMA CVD Programme are provided "as is", without any warranty of any kind.

All warranties, whether expressed, implied, or statutory, including without limitation any implied or other warranties of merchantability, fitness for a particular purpose, non-infringement, quality, accuracy, completeness, title or quite enjoyment are expressly disclaimed and excluded.

As this Programme is designed to benefit the safety of mobile networks and users, the CVD Governance Team, the GSMA, its staff and Members do not warrant or assume any liability for the responsibilities of this Programme, or "Validation of Submissions" and any other activities or milestones set forth by the GSMA.

Each beneficiary of this activity will engage in this offering without reliance or any representation and/or warranty of the other parties and all such representations and/or warranties are, to the greatest extent permitted by applicable law, hereby disclaimed.

Owners or providers of an offering that has been identified by a Finder as having a vulnerability will only be given details of such vulnerability under this Programme. The vulnerability must be validated in accordance with the GSMA CVD process.

Applying to join the CVD Panel of Experts

Applications to join the GSMA CVD Panel of Experts (PoE) happen once a year. To register interest for the next recruitment exercise please click on the Application Form link at the bottom of this page and return it to **cvd@gsma.com**

The GSMA CVD PoE is the group of subject matter experts from GSMA Operator, Associate and Rapporteur Members who assess and consider options for remediation of vulnerabilities submitted to GSMA. PoE activities include technical analysis, assessing the impact of submission, suggesting remediation options, and contributing to advisories relating to the vulnerability. They also review the GSMA CVD Programme.

The GSMA CVD scope is security vulnerabilities that impact the mobile industry, primarily open standards-based technologies. We therefore work with a broad cross-section of the industry to consider and develop remediations for vulnerabilities which are submitted to us.

Benefits for individuals joining the CVD PoE include:

- Gaining professional fulfilment from supporting the whole mobile industry
- The opportunity to consider and develop remediating and mitigating actions for interesting and varied mobile security vulnerabilities
- Insight to coordinated vulnerability disclosure

GSMA Operator, Associate and Rapporteur Members interested in applying to join the **CVD Panel of Experts** can find details in the next section.

Individuals wishing to apply to join the CVD PoE need to be able to commit to support the industry Programme, read and understand how the GSMA CVD Programme works and in particular the role of the CVD PoE in this, and have the backing of their employer to allow them to take part. Successful applicants are required to join a training e-meeting before taking part in discussions about CVD submissions.

CVD Panel of Expert Companies

- Apple
- AT&T
- Copper Horse
- Deutsche Telekom
- Ericsson
- Giesecke+Devrient Mobile Security GmbH
- Huawei
- Idemia
- Nokia
- NTT DOCOMO
- Orange
- Qualcomm
- Swisscom
- TIM
- T-Mobile US
- U-Blox
- Umlaut Communications Gmbh.
- Vodafone
- ZTE

*Correct as of 28/05/2024.

“If you have a drive to make a positive impact for the telecom security ecosystem and you have the capacity to understand the standards and the academic research papers then of course come and join!”

Prajwol Nakarmi,
Strategic Product Manager for RAN Security at Ericsson

GSMA Mobile Security Research Acknowledgements

The GSMA's Mobile Security Research Acknowledgements page lists security vulnerability reporters that have made contributions to increasing the security of the mobile industry by submitting disclosures to the GSMA or its Members. It is the primary mechanism for the GSMA to recognise and acknowledge the positive impact the reporter has had on the mobile industry by following the GSMA's CVD process. This was previously known as GSMA Mobile Security Hall of Fame from 2017 - May 2021.

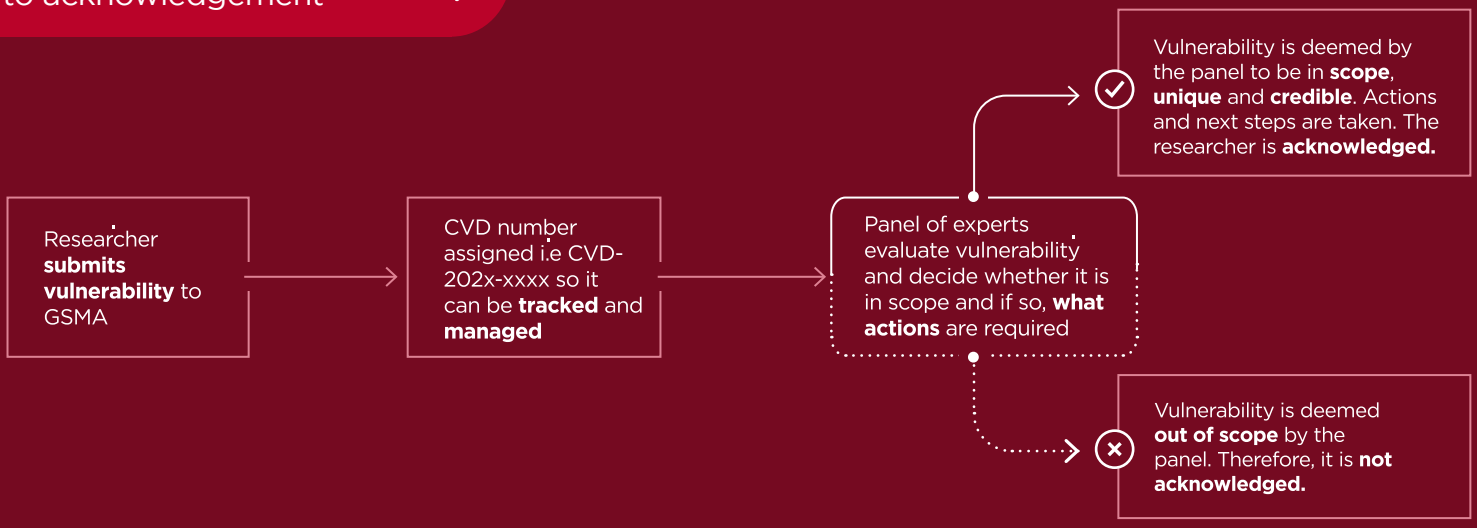
Does a CVD number signify an acknowledgement?

The GSMA's CVD Programme assigns CVD numbers to facilitate the tracking and management of each case.

The allocation of a CVD number does not imply that the panel of experts has assessed or publicly acknowledged the research.

After the assignment of a CVD number, the panel of experts reviews the vulnerability and determines whether the research is in scope, unique and credible and establishes the appropriate next steps and actions. If the research is deemed in scope, unique and credible, the researchers are acknowledged on the list below, once mitigating actions have been undertaken by GSMA.

GSMA CVD process flow to acknowledgement



This Mobile Security Research Acknowledgements page also facilitates the nomination and recognition of other reporters of vulnerabilities that may have made significant discoveries of vulnerabilities to individual GSMA Member companies.

Entry to the Mobile Security Research Acknowledgements page is optional and is at the discretion of the reporter, the GSMA and/or the nominating GSMA Member.

There are two ways of submitting to the GSMA CVD Programme. You can download the submission form in Microsoft Word or Text version format and send it back to the GSMA, or you can fill the **online form below**.

We request reporters of vulnerabilities to describe the vulnerability on the submission form, including:

- Identification of the vulnerable target(s)
- A description of the vulnerability
- Operations carried out to exploit the vulnerability

How to submit research

This is usually sufficient information to enable the GSMA to consider the vulnerability and will allow for verification and identification of possible remediations. A proof-of-concept (POC) or more detailed description may be requested in the case of complex vulnerabilities.

The GSMA may ask a Reporter for more information throughout the consideration process.

Researcher Testimonial: Find out what the importance is of submitting a vulnerability to the CVD Programme, the experience of working with the GSMA and the additional benefits of engagement with the mobile industry.

Submission forms

Submission form – Word version

Submission form – Text version

Once you have completed this template, you should submit it by email to the GSMA on **security@gsma.com**.

The GSMA recommends that all vulnerability disclosure submissions are encrypted, but use of encryption is at the discretion of the Finder.

Click here to view the CVD submission process.

Scope

Is the GSMA's CVD Programme the correct scheme to bring my research to?

The scope of the GSMA CVD Programme is security vulnerabilities that impact the mobile industry, primarily open standards-based technologies.

The following items are out of scope for the CVD Programme:

- Research or information on a vulnerability which has previously been made public. Research or information on a vulnerability which is already in the public domain is out of scope for inclusion in the Acknowledgements page, but may be considered through the CVD Programme in order to develop remediations.
- Services or products provided by a single manufacturer or manufacturer group – these should be reported to the relevant manufacturer.
- Services or products provided by a single company or group of companies. These should be reported to the relevant company.
- Submissions by GSMA Members, Associate Members and Rapporteurs where they are working on the topic as part of an Activity. These should be reported through the relevant Activity apart from in the case of exceptional circumstances.

For vulnerabilities affecting one manufacturer or network, please contact them directly – some vulnerability disclosure programmes from **GSMA Members can be found here.**

For reporting vulnerabilities in GSMA websites or services please see **here**.

Research expectations

The GSMA is grateful to Reporters who afford us the opportunity to consider their findings, liaise with the industry and define remediation and mitigation actions. However, participation in the CVD Programme requires that Reporters do not engage in activities that violate any local legislation or regulations and third-party rights.

Reporters are asked to:

- Not abuse the reported vulnerability. For example, downloading more data than is necessary to demonstrate the vulnerability, or changing/deleting live systems, settings or data.
- Exercise caution and restraint with regard to personal data and not intentionally engage in attacks against third parties, social engineering, denial-of-service attacks, spamming or otherwise cause a nuisance to other users.

If there is any doubt, please contact **security@gsma.com**.

PGP DETAILS:

Comment: Created: 27/07/2023
Comment: Expires: 27/07/2026
Comment: Type: 2048-bit RSA (secret key available)
Comment: Usage: Signing, Encryption, Certifying User-IDs
Comment: Fingerprint: 22150430A5020646BEF798B426B-19DAC4B3DE074

—-BEGIN PGP PUBLIC KEY BLOCK—-
mDMEZMJsshYJKwYBBAHaRw8BAQdABaTG0DOU2wffeJCa-ZpZ36VpCD5yx9v5DObSDfJx/U7O0IFIgQnJvd24gMjMgTkVX-IDxyYnJvd25AZ3NtYS5jb20+iJkEExYKAEEWIQQiFQQwpQI-GRr73mLQmsZ2sSz3gdAUCZMJssgIbAwUJBaTNfgULCQgH-AgIiAgYVCgkICwIEFgIDAQIeBwIXgAAKCRAmsZ2sSz3gdHtu-AQDhrJhOU1vwVlht5rDbY1Vo
s1wH/VRtrUTTdrNWf5c83gD+JsWNanRC0YqQjDXL3WT-KpclHvv00n3YTBlPpyqLLCw+4OARkwmyyEgorBgEEAZd-VAQUBAQdAQWoeEk/CMdWa1Cvf0eD74hqC+Pe/4ANRXX-2gDmvQ+TQDAQgHiH4EGBYKACYWIQQiFQQwpQIGRr73m-LQmsZ2sSz3gdAUCZMJssgIbDAUJBaTNfgAKCRAmsZ2sSz3g-dP7sAQCoYcQnm3p3gxTrzIyOkeABEHU2xfaGjpacHif5XsddO-QD+LnnyYKuxOzFStSRQCmB91rZOlke1n3EtOeAgwmz1cQA=
=ljkl
—-END PGP PUBLIC KEY BLOCK—-

GSMA Members' vulnerability disclosure programmes

Please see below our directory of GSMA Member companies which may also have their own vulnerability disclosure programmes. The GSMA is not responsible for the vulnerability disclosure process of Member companies.

Please see guidance the GSMA has put together about **setting up a CVD Programme**.

The **GSMA's industry CVD Programme** considers vulnerabilities affecting open standards-based technologies which are not proprietary to a specific vendor but that are used across, or have significant impact on, the mobile industry. The GSMA also has its own disclosure process for vulnerabilities affecting **GSMA assets or services**.

CVD Programme – GSMA assets

The GSMA recognises the value and potential for coordinated vulnerability disclosure to facilitate the reporting and remediation of security vulnerabilities. It welcomes disclosures pertaining to its own product or service offerings and its technology assets, including those below.

Please note: recognition in the **Mobile Security Research Acknowledgements page** is for identifying vulnerabilities which affect mobile industry standards and services, NOT for those pertaining to GSMA assets listed below.

This is not a bug bounty programme - consequently the GSMA does not offer any rewards for submitted vulnerabilities of this type.

- GSMA websites
- InfoCentre
- Device Database
- Device Check
- Device Map
- Pathfinder
- Event systems and services
- RAEX
- Pegged Exchange

We invite private individuals and organisations to report vulnerabilities identified in GSMA assets.

GSMA Head Office
1 Angel Lane
London EC4R 3AB
United Kingdom
Tel: +44 (0)20 7356 0600
Fax: +44 (0)20 7356 0601