GLOBALPLATFORM®
THE STANDARD FOR SECURE DIGITAL SERVICES AND DEVICES

GlobalPlatform Technology

Vulnerability Disclosure and Mitigation Process

Version 1.0

Public Release

September 2020

Document Reference: GP_PRO_066

Contents

Figures

Tables

1 Introduction

The ISO 27000 family addresses security management required to deal with vulnerabilities through defined procedures. This document outlines GlobalPlatform's implementation of those procedures. Independent of the urgency to deal with a vulnerability, it is important to treat it in a structured manner. Change management or incident response procedures should be considered to treat vulnerabilities, because they can provide guidance on what to do considering prioritization, response time, response escalation, etc.

As a security standards organization, GlobalPlatform is committed to receiving and responding to reports of potential vulnerabilities in, for example, specifications, reference code, and reference documents.

The aim of this document is to define how GlobalPlatform accepts and manages the disclosure of vulnerability on GlobalPlatform technology.

1.1 Audience

This document is intended primarily for the use of developers, vendors, evaluators, and users of GlobalPlatform technology, GlobalPlatform members, and anyone that wants to disclose vulnerabilities to GlobalPlatform.

1.2 IPR Disclaimer

Attention is drawn to the possibility that some of the elements of this GlobalPlatform specification or other work product may be the subject of intellectual property rights (IPR) held by GlobalPlatform members or others. For additional information regarding any such IPR that have been brought to the attention of GlobalPlatform, please visit https://globalplatform.org/specifications/ip-disclaimers/. GlobalPlatform shall not be held responsible for identifying any or all such IPR, and takes no position concerning the possible existence or the evidence, validity, or scope of any such IPR.

1.3 References

The table below lists references applicable to this specification. The latest version of each reference applies unless a publication date or version is explicitly stated.

Table 1-1: Normative References

Standard / Specification	Description	Ref
ISO 29147	Information technology — Security techniques — Vulnerability disclosure	[ISO 29147]
ISO/IEC 27000	Information technology — Security techniques — Information security management systems — Overview and vocabulary	[ISO 27000]
ISO 30111	Information technology — Security techniques — Vulnerability handling processes	[ISO 30111]

1.4 Terminology and Definitions

Table 1-2: Terminology and Definitions

Term	Definition
Reporter	Expert that notifies GlobalPlatform of a potential vulnerability

1.5 Abbreviations and Notations

Table 1-3: Abbreviations and Notations

Abbreviation / Notation	Meaning
CD	Certification Director
CVSS	Common Vulnerability Scoring System
ED	Executive Director
PGP	Pretty Good Privacy
SIRT	Security Incident Response Team
SME	Subject-Matter Experts
TD	Technical Director

1.6 Revision History

GlobalPlatform technical documents numbered *n*.0 are major releases. Those numbered *n*.1, *n*.2, etc., are minor releases where changes typically introduce supplementary items that do not impact backward compatibility or interoperability of the specifications. Those numbered *n.n*.1, *n.n*.2, etc., are maintenance releases that incorporate errata and precisions; all non-trivial changes are indicated, often with revision marks.

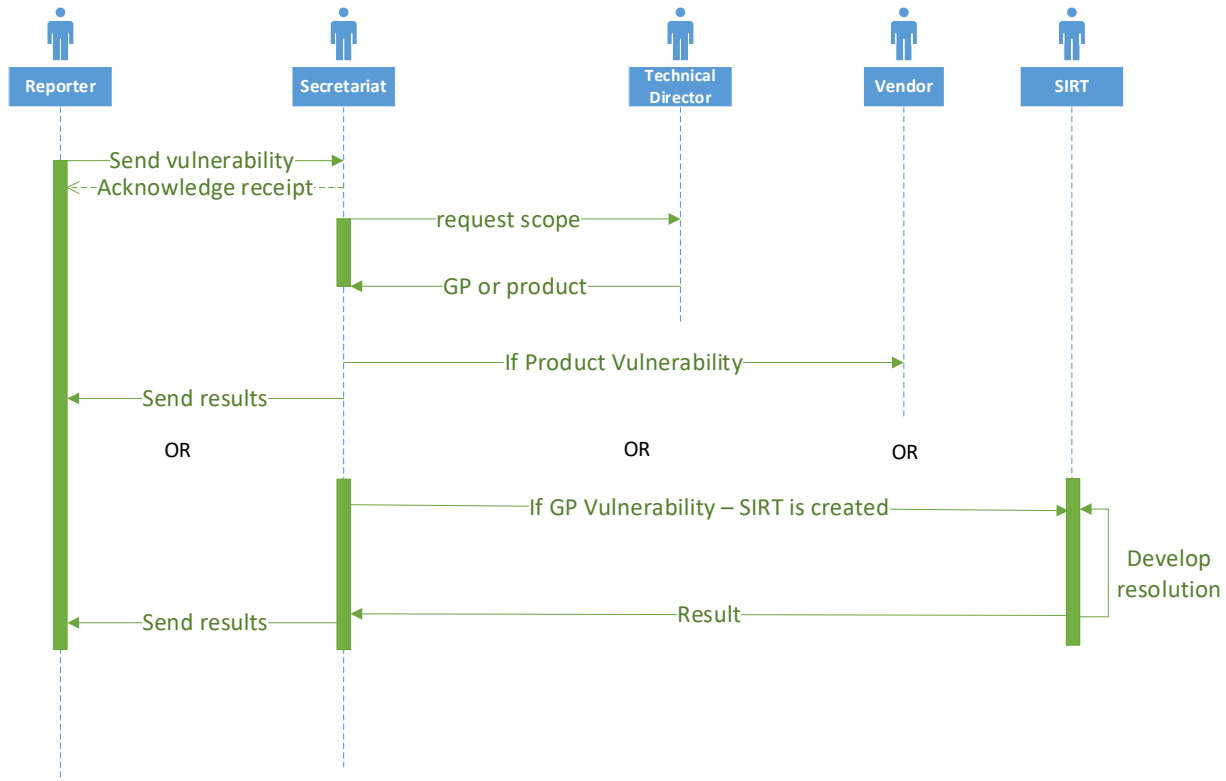
Table 1-4: Revision History

Date	Version	Description
September	1.0	Public Release

2 Overview

The term “vulnerability disclosure” is used to describe the overall activities associated with receiving vulnerability reports and providing remediation information.

Figure 2-1: Process Overview



2.1 Reporting

GlobalPlatform can receive or monitor for notification of potential vulnerabilities from various sources: internal discovery, monitoring, public disclosure, or through a vulnerability reporting source.

Vulnerabilities should be reported by sending an encrypted email to vulnerability@globalplatform.org using the current PGP public key for the vulnerability, available in the GlobalPlatform public web site at https://globalplatform.org/specifications/vulnerability-disclosure/. Unencrypted plaintext email can be received, but it is discouraged.

Initial receipt of the submission, via email, will be acknowledged within 72 hours.

The GlobalPlatform Secretariat sends an acknowledgement to the Reporter.

In order to ensure that GlobalPlatform will accept the vulnerability report, the Reporter should use the template defined in Annex A to create the vulnerability report.

2.2 Preliminary Verification

The GlobalPlatform Secretariat requests the Technical Director to check if the vulnerability applies to GlobalPlatform technology. In case of obvious product vendor vulnerability the secretariat may proceed directly without Technical Director advice.

If the vulnerability applies to a specific product or implementation of GlobalPlatform technology in a product, the report will be forwarded to the product's vendor using the vendor's vulnerability process. In this case the secretariat will inform the Reporter that the vulnerability has been forwarded to the vendor and the incident is closed.

If the vulnerability applies to a GlobalPlatform technology, a Security Incident Response Team (SIRT) will be created with at least the Chair of the committee maintaining the affected specification, Security Task Force chair, Executive Director (ED), a representative from the GlobalPlatform press agency, Technical Director, and Certification Director (CD).

The board will be informed of the creation of the SIRT and may nominate individuals from their own organizations to participate. Nominees who have experience with product security incident response or cybersecurity incident response are preferred. Nominees are expected to be incident managers, not Subject-Matter Experts (SMEs). They may happen to have both skillsets, but SIRT members are primarily expected to contribute to incident response activities, not subject-matter consultation.

The group will elect a chair; this position may be also managed by the ED, CD, or TD.

The SIRT will use a common PGP Key to protect all information shared during incident management. If possible, this key is not reused for incidents in different committees and is renewed every two years.

The first action of the SIRT is to assess the level of severity of the disclosure: None, Low, Medium, High, or Critical. If the level of severity of the disclosure is High or Critical, specific deviation of the current publication rules (for example number or duration of review period) will be proposed to the board for agreement.

2.3 Remediation Development

The SIRT determines how the vulnerability can be remediated comprehensively, how to reduce the impact of successful exploitation of the vulnerability, or how to reduce exposure.

During this phase, the need for technical consultation with specific work group participants is expected. In such circumstances, the SIRT needs to reach beyond their own membership into specific areas of expertise within GlobalPlatform by consulting with appropriate work group participants. SMEs are expected to provide consultation, not incident-response services. Such interactions will likely need higher levels of confidentiality and sensitive handling beyond standard levels of confidentiality within the usual GlobalPlatform activities. The SIRT chair then contacts that SME, informs the SME about the issue, explains the guidelines and constraints, and then proceeds with consultation.

The Reporter may also be invited to participate during this remediation development phase.

Depending on the vulnerability, remediation may cover the following:

- Development of the specification with a corrective solution
- Affected feature moved to obsolete status
- Archive of the specification
- Publication of a Security Note to inform GlobalPlatform users

In the event that legal consultation or external expertise is needed, the SIRT chair will request approval of expenditure from Board Officers. Special considerations include emergency or time sensitive situations as determined by the SIRT. Because events occur rapidly in an incident, the board may consider preauthorizing some basic level of funding.

The SIRT should choose an appropriate date for public vulnerability disclosure and prepare the advisory with the assistance of the product business division and other major stakeholders, such as legal, public relations, and external coordinators, if applicable. The vulnerability disclosure should align with when the remediation is available so that users can take the necessary action immediately.

2.4 Release

Based on the SIRT guidance, the GlobalPlatform Secretariat will publish the results in the GlobalPlatform website and inform the Reporter of the incident outcome.

2.5 Post Release

The secretariat is responsible for ensuring that a report is created and provided to the board, to enable them to monitor the effectiveness of their vulnerability handling processes, including but not limited to the following measurements:

- Speed: The time it takes to address a vulnerability through this process and strive toward improving the speed of vulnerability remediation. If the risk level of the vulnerability is high, the rapid remediation of the vulnerability can help to limit the damage spreading.
- Completeness: The completeness of the remediation, to ensure that it addresses the root cause of the vulnerability. However, if urgency is required in order to address a vulnerability that is already being exploited, vendors may create a less complete remediation as a temporary measure, and this should be taken into consideration when monitoring this aspect of the vulnerability handling processes.
- Effectiveness: The number of requests from GlobalPlatform users after the release of the remediation.

Annex A Vulnerability Report Information

Include the following information in the Vulnerability Report:

- Reporter's email
- Short Description
- Vulnerability Description (include vulnerability details and how to reproduce the issue)
- The version label for the affected software or document
- Vendor(s) known to be affected
- Any known exploits
- Attachments
- Reporter's PGP public key (if not already known or if not already available via standard means)
- Reporter's estimated CVSSv3 score and vector
- Previously disclosed (Y/N – if Y, provide where & when)
- Disclosure planned (Y/N – if Y, provide where & when)