



VULNERABILITY COORDINATION POLICY

v1.0

2010-01-08



Introduction

CERT-FI is the Finnish national Computer Emergency Response Team within the Finnish Communications Regulatory Authority (FICORA). The task of CERT-FI is to promote security in the information society by preventing, observing and solving information security incidents and disseminating information on threats to information security.

In CERT-FI's view software vulnerabilities pose a serious threat to the normal functioning of information society. It is self-evident that vulnerabilities need to be identified before they can be satisfactorily fixed or the threat posed by them can otherwise be mitigated. Furthermore, it has been seen that using software testing methodologies and employing security research approaches can help identify previously unknown vulnerabilities. The findings, however, need to be handled in a responsible manner as the findings may have far-reaching adverse consequences to the people's privacy, possessions and business, and they may even affect national security.

In its role as a vulnerability coordinator, CERT-FI promotes responsible handling of vulnerability information during all stages of the vulnerability lifecycle, not merely during the disclosure phase. It is not enough that the vulnerability is identified. The weaknesses that the vulnerability attributes to need to be fixed, the fixes need to be delivered to the user community and they need to be applied in order to be of value. Coordinators aim to strike a balance between the interests of the vulnerability discoverers, software vendors and integrators and the end-user community by ensuring that as many vulnerabilities as possible will eventually be fixed and the fixes will be applied.

Goals

It is the goal of CERT-FI to reduce or totally eliminate harmful effects of software vulnerabilities. This is achieved by providing vulnerability coordination services to the benefit of various parties, most notably vulnerability discoverers, software vendors, systems integrators as well as end-users. The public's right to be informed about security vulnerabilities has to be balanced with the vendors' process and business needs, and the security needs of the affected end users. In this process, CERT-FI aims to work as a trusted intermediary between the vulnerability discoverers, affected vendors and the public.

Initiating vulnerability coordination

The coordination process is typically initiated by the original discoverer reporting (later referred to as the Reporter) the vulnerability to the CERT-FI and requesting assistance in contacting the vendors or informing the affected parties.

Two conditions must be successfully satisfied before CERT-FI accepts the responsibility of a vulnerability coordination project.

1. the Reporter and CERT-FI must reach a mutual understanding of the coordination project and its goals.
 - Details such as project phasing and the rules for pre-disclosure handling of the potentially sensitive vulnerability details must be covered.
 - The scope of the eventual disclosure must be agreed. A shared view of the intended outcome for the project has proven to be vital to its successful execution.
2. The vulnerability finding must be significant enough to warrant coordination efforts by CERT-FI.
 - Coordination projects are prioritised based on the estimated vulnerability impact, current threat situation and the resource constraints of CERT-FI.
 - Vulnerabilities that affect a large number of vendors and a wide array of products are prioritised for coordination.
 - Vulnerabilities affecting a large number of users or critical infrastructures are generally concerned eligible, provided that coordination by CERT-FI provides added value.
 - Vulnerabilities that are trivial in nature or that only affect a limited amount of users or implementations may be deemed ineligible for coordination.

CERT-FI uses the vulncoord@ficora.fi email address for vulnerability-related communication. PGP keys for this address are available at:

<https://www.cert.fi/en/activities/contact/pgp-keys.html>.

Schedule of publication

If possible, the schedule of publication of the vulnerabilities reported to the CERT-FI will be negotiated with the affected vendors. If the vendor cannot be reached or mutual understanding on the disclosure schedule cannot be found, information about the vulnerabilities will be made public 42 days after the initial report, regardless of the existence or availability of patches or workarounds from affected vendors.

The final determination of a publication schedule will be, however, decided case-by-case. Changes in circumstances, such as active exploitation, threats of an especially serious (or non-trivial) nature, or situations that require changes to an established standard may result in rescheduling.

Contacting the vendors

CERT-FI will aim at sharing vulnerability details with the affected vendors as soon as practical after report receipt. Contacts will be made by using the product security contacts as provided by the vendor. Vendors will be given five business days to reply to the first contact.

If no contact can be established, the vendor risks being left out of further information exchange. Also, disclosure of vulnerability details may be expedited if vendor's non-responsiveness is deemed to pose a security threat to the affected end-users.

CERT-FI reserves the right to use trusted third parties such as other coordinators and CERT teams to relay vulnerability information to vendors. CERT-FI may also alert trusted third parties prior to the publication of vulnerability information.

Whenever possible, all vendor communication will be encrypted via PGP or S/MIME to protect the sensitive nature of the information during transit.

Vulnerability management standards

CERT-FI will ensure the acquisition of CVE numbers for vulnerabilities accepted for coordination.

Credits

As a general rule, CERT-FI will credit the Reporter unless otherwise requested.

Providing exploits and vulnerability analysis

No exploits for vulnerabilities will be published by CERT-FI, not even for demonstration purposes. Due to resource constraints, vulnerability analysis will be performed only if so requested by a priority partner or if the impact of the vulnerability in question is significant.

Legal notice

The imperative legislation in Finland, most notably Act on the Openness of Government Activities (621/1999), may in some cases set some boundary conditions for the processing and publication of the vulnerability information.

CERT-FI is tasked by law to collect information on and investigate threats to information security in public communications networks and services. The duties of CERT-FI have been described in Section 31 of the Act on the Protection of Privacy in Electronic Communications (516/2004).

Definitions

Vulnerability A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy.¹

Exploit Colloquially for exploit script: a script, program, mechanism, or other technique by which a vulnerability is used in the pursuit or achievement of some information assurance objective. It is common speech in this field to use the terms exploit and exploit script to refer to any mechanism, not just scripts, that uses a vulnerability.²

Additional material

This policy has been modeled after and in collaboration with CERT/CC. Their Vulnerability Disclosure Policy can be found at:

<http://www.kb.cert.org/vuls/html/disclosure>

A collection of other vulnerability disclosure policies and guidelines can be found at the Oulu University Secure Programming Group's (OUSPG) web page.³

¹ IETF, RFC 2828, <http://www.ietf.org/rfc/rfc2828.txt>

² Carnegie Mellon, Software Engineering Institute, State of the Practice of Intrusion Detection Technologies, <http://www.sei.cmu.edu/reports/99tr028.pdf>

³ OUSPG, Disclosure policies and Guidelines, https://www.ee.oulu.fi/research/ouspg/Disclosure_tracking#Disclosure_policies_and_Guidelines