‹RFC 2350›

/ Description of EmbedIT CSIRT

About this document

This document is a description of the EmbedIT CSIRT team with standard RFC 2350. It provides basic information about EmbedIT CSIRT and EmbedIT s.r.o., possibilities of contact, responsibilities and services provided.

Date of last update

This is version 1 published 14 April 2026.

Distribution List for Notifications

There is no distribution list for notifications. Any specific questions or remarks please address them to the EmbedIT CSIRT team mail address.

Location where this document may be found

The latest version of this CSIRT description document is available from this location: https://www.embedit.com/cybersecurity

Contact information

Team Name

EmbedIT CSIRT

Address

EmbedIT CSIRT

EmbedIT s.r.o.

Evropská 2690/17

160 00 Prague 6 – Dejvice

Time Zone

GMT +0100 – Central European Time (CET)

GMT +0200 – Daylight Saving Time (from the last Sunday in March to the last Sunday in October)

Telephone Number

+420 601 073 530

Telephone number is available on working days from 9 a.m. to 5 p.m.

Facsimile Number

None available

Other Telecommunication

None available

Electronic Mail Address

For all communications towards EmbedIT CSIRT, including incident reports, use the address csirt@embedit.com.

Public Keys and Encryption Information

For encrypted communication with EmbedIT CSIRT, you may use the following key:

UID: EmbedIT CSIRT (EmbedIT CSIRT) csirt@embedit.com

Key fingerprint: 0F8F 3428 78C1 1721 3041 08D8 3BC7 D1DB 8896 1D38

Public key is downloadable from: https://keys.openpgp.org/vks/v1/by-fingerprint/0F8F342878C11721304108D83BC7D1DB88961D38

Team Members

The manager of EmbedIT CSIRT is Jiří Běhal. The full list of team members is not publicly disclosed.

Other Information

General information about EmbedIT CSIRT can be found at https://www.embedit.com/cybersecurity

Points of Customer Contact

Preferred way to contact EmbedIT CSIRT is via email at csirt@embedit.com, where a responsible team member will process incoming requests.

If it is not possible (or not advisable for security reasons) to use e-mail, the EmbedIT CSIRT can be reached by telephone.

The EmbedIT CSIRT hours of operation are generally restricted to regular business hours (09:00 – 17:00 Monday to Friday, except holidays). An on-call service is provided outside of working hours.

Charter

Mission statement

EmbedIT CSIRT handles cybersecurity incidents for EmbedIT s.r.o. and EmbedIT s.r.o. customers with whom a service agreement has been concluded. Our goal is to help them effectively address security challenges, respond to incidents, coordinate steps to resolve them, and effectively prevent them.

Constituency

Constituency of EmbedIT CSIRT are EmbedIT s.r.o. and customers of EmbedIT s.r.o. with whom a service agreement has been concluded.

Sponsorship and/or Affiliation

EmbedIT CSIRT is a part of the Cyber Security Department of EmbedIT s.r.o. (part of PPF Group).

Authority

EmbedIT CSIRT has a mandate from the management of EmbedIT s.r.o. to manage the lifecycle of security incidents.

EmbedIT CSIRT excepts to work in close cooperation with the government CERT of the Czech Republic and other CERT/CSIRT teams depending on the specific nature and needs of the incident.

Policies

Types of Incidents and Level of Support

EmbedIT CSIRT is authorized to handle all types of security incidents that have occurred or may occur within its constituency.

The level of support provided by EmbedIT CSIRT varies depending on the type and severity of the incident, the nature of its origin, the size of the affected user community, and the availability of resources at the time of the incident, however some type of response will be provided in every case.

Please note that no direct support will be given to end users; they are expected to contact their system administrator, network administrator or security managers for assistance. EmbedIT CSIRT will provide support to these responsible individuals.

EmbedIT CSIRT is committed to keeping its constituency informed of potential vulnerabilities, and where possible, will inform this community of such vulnerabilities before they are actively exploited.

Co-operation, Interaction and Disclosure of Information

EmbedIT CSIRT is ready to cooperate with another trusted security teams (CERT/CSIRT) in the Czech Republic or abroad.

EmbedIT CSIRT follows internal data handling and data protection policies/guidelines. Information may be shared with trusted parties on a need-to-know basis and solely for purpose of incident resolution.

EmbedIT CSIRT operates within the bounds of the Czech and EU legislation.

Communication and Authentication

For regular communication that does not contain sensitive information, email can be used. For secure communication, encrypted email using PGP key is required.

Services

Incident Response

EmbedIT CSIRT team aims to provide support and assistance in managing security incidents to customers of EmbedIT s.r.o. EmbedIT CSIRT handles all technical and organizational aspects of incident response. In particular, it provides the following services:

Incident triage

The primary objectives of incident triage are:

- Investigating whether a security incident has actually occurred,
- Assessing the scope and severity of the incident.

Incident Coordination

The goal of incident coordination is to:

- Identify the initial cause of the incident (exploited vulnerability),
- Contact the parties involved in the incident to investigate the incident and subsequently take appropriate measures,
- Facilitate a contact with other entities than can assist in resolving the incident,
- Inform other CERT and CSIRT teams if necessary,
- Communicating with the parties involved,

Incident resolution

The following measures will be taken as part of the incident resolution:

- Removing the vulnerability,
- Securing the system from the effects of the incident,
- Collecting evidence and data interpretation

Proactive activities

EmbedIT CSIRT participates in activities focused on:

- Raising security awareness in its constituency,
- Issuing public announcements concerning significant security threats,
- Monitoring current trends in technology and security,
- Distribute relevant knowledge to its constituency.

Incident reporting form

There are no specific forms available for reporting incidents. When reporting incidents via email, please follow these steps:

- A report must contain your contact and organizational function – first name and last name of the reporter, organization name (if applicable), email and telephone number,
- A report must contain IP address and type of the incident, approximate time when the incident started, when the incident was detected, and logs relevant to the problem (where applicable)
- A report about spam (or a malicious e-mail attachment) must contain a copy of the full e-mail header from the e-mail which is considered to be spam (or which contains the attachment in question),
- A report about phishing or pharming must contain the URL and IP address of the web page along with its source code, if possible.

Disclaimer

While every effort will be made to ensure the accuracy of information, notifications and alerts, EmbedIT CSIRT assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.