Information on GovCERT

By Federal Department of Defence, Civil Protection and Sport DDPS

Archived: 2026-04-10 03:13:58 UTC

Information on GovCERT

The Government Computer Emergency Response Team (GovCERT) is the national specialist service responsible for the technical management of cyberincidents and technical analysis of cyberthreats. It supports critical infrastructure operators, the public sector and the Swiss business location with technical information on current cyberthreats and with the management of cyberincidents. GovCERT also works in close collaboration with the police authorities. This cooperation covers both the exchange of information and support with technical analyses.

To ensure the timely exchange of information on cyberthreats, GovCERT works with other CERTs and CSIRTs (computer security incident response teams) worldwide. In addition, GovCERT is a member of various recognised international organisations.

- Blog and white papers
- List of blocked file types
- International cooperation
- Contacts
- GovCERT on Twitter/X

Blog and white papers

Over the years, GovCERT has published a variety of blogs, white papers (technical reports) and other documentation on cyberthreats (previously on www.govcert.ch).
These documents will now be published on GitHub:

List of blocked file types

GovCERT publishes a list of file types that are often used to distribute malware by email, and recommends that these be proactively blocked at the email gateway or spam filter, or placed in quarantine.

International cooperation

In the joint fight against cyberthreats, international cooperation is very important. Membership in various associations enables GovCERT to establish a global network of personal relationships. GovCERT is a member of FIRST (Forum of Incident Response and Security Teams, www.first.org), of the European Government CERTs (EGC) group (www.egc-group.org) and of the International Watch and Warning Network (IWWN). In addition, GovCERT has accreditation from the European Trusted Introducer (TI) Service.

Contacts

Reports on cyberincidents from critical infrastructures

Reports on cyberincidents from critical infrastructures or cybersecurity specialists can be sent to GovCERT at the following email address:

incidents[at]govcert{dot}ch

Technical queries

Other technical queries that do not concern a specific cyberincident can be sent to GovCERT at the following email address:

outreach[at]govcert{dot}ch

Encryption Keys

These two GovCERT mailboxes support PGP and S/MIME, which allow secure and phishing-resistant email communication. The
corresponding keys can be found here:

Expectations for cyberincident management

GovCERT publishes the expectations for cyberincident management in accordance with RFC 2350 ("Expectations for Computer Security Incident Response"):

General reports on cyberincidents

General reports on cyberincidents can be sent to the NCSC using the web form. This helps the NCSC to identify potential online threat trends and take targeted action to combat them:

NCSC reporting form

GovCERT on Twitter/X
