RFC 2350 MIL.CERT-UA – the CERT for the defence sector in Ukraine

• Date of last update

This is version 1.0, published on 28th March 2025

• Distribution list for notifications

Currently MIL.CERT-UA does not use any distribution lists to notify about changes in this document.

• Locations where this document may be found

The current version of this description document is not available publicly, web site is under development.

• Authentication this document

This document has been signed with the MIL.CERT-UA PGP key. The signature is also on our web site, under: milcert.mod.gov.ua

• Name of the team

MIL.CERT-UA – Military Computer Emergency Response Team Ukraine, the CERT for the defence sector

• Address

MIL.CERT-UA
Povitrianykh Syl Ave, 6, Kyiv, 03168, Ukraine

• Telephone number

+38 096 773 73 70

• Electronic mail address

Incident reports, notifications, cooperation requests and other related correspondence should be sent to cert@mil.ua

• Public keys and other encryption information

MIL.CERT-UA has an OpenPGP public key, which KeyID is 0x9669A693 and fingerprint is: A98B 426E F0AE C53C F167 1128 148E 0E3A 9669 A693
pub 4096R/9669A693 2025-03-25 Key fingerprint = A98B 426E F0AE C53C F167 1128 148E 0E3A 9669 A69 uid MIL.CERT-UA cert@mil.ua sub 4096R/E1B5F505 2025-03-25

- **Team members**

MIL.CERT-UA is the CERT for the defence sector of Ukraine. MIL.CERT-UA is operated by Cyber Incident Response Centre Ministry of Defence of Ukraine, designed to improve information security and create new opportunities for Ministry of Defence of Ukraine and Defence Forces of Ukraine.

The head of MIL.CERT-UA is Col. Deny Petrov.
Information about other team members is available by request.

- **Other information**

The preferred method for contacting MIL.CERT-UA is via e-mail at cert@mil.ua. We encourage our constituency (customers) to use PGP encryption when sending any sensitive information to MIL.CERT-UA.
If it is not possible (or not advisable for security reasons) to use e-mail, MIL.CERT-UA can be reached by Signal or telephone in any time.
MIL.CERT-UA hours of operation are 24/7/365.

- **Mission statement**

MIL.CERT-UA is the CERT for the defence sector of Ukraine. MIL.CERT-UA is operated by Cyber Incident Response Centre Ministry of Defence of Ukraine, designed to improve information security and create new opportunities for Ministry of Defence of Ukraine and Defence Forces of Ukraine.

Its missions are to:

- Taking measures of operational (crisis) response to cybersecurity incidents and exercising operational control during their conduct;
- taking measures for the cyber defence of information and communication systems (except for the MoD intelligence agency);
- implementing and ensuring the functioning of the following in the MoD system:
    - cybersecurity incident management system;
    - cyber threat information exchange system;

- interacting with the relevant units of the main actors of the national cybersecurity system and the defence forces in terms of jointly performing cybersecurity tasks;
- organising and conducting practical cybersecurity exercises to increase the level of cyber awareness of users;
- military cooperation with NATO and other defence actors to ensure cyberspace security and joint defence against cyber threats.

Constituency

MIL.CERT-UA is the CERT for the Defence Forces of Ukraine. MIL.CERT-UA is operated by Cyber Incident Response Centre Ministry of Defence of Ukraine.

Sponsorship and/or Affiliation

MIL.CERT-UA is the CERT for the Defence Forces of Ukraine. MIL.CERT-UA is operated by Cyber Incident Response Centre Ministry of Defence of Ukraine, designed to improve information security and create new opportunities for Ministry of Defence of Ukraine and Defence Forces of Ukraine.

MIL.CERT-UA is state funded by Ministry of Defence of Ukraine.

Authority

MIL.CERT-UA operates by Cyber Incident Response Centre Ministry of Defence of Ukraine, by order of Minister of Defence.
Information for ASN can be provided by request.

Types of incidents and level of support

MIL.CERT-UA is authorized to address all types of computer security incidents which occur, or threaten to occur, in the structure of the Ministry of Defence of Ukraine networks.
The level of support given by MIL.CERT-UA will vary depending on the type and severity of the incident or issue.
Incidents will be prioritized according to their apparent severity and extent.
End users are expected to contact their systems administrator, network administrator, or department head for assistance.

Cooperation, interaction and disclosure of information

MIL.CERT-UA exchanges all necessary information with other CERTs as well as with affected parties' administrators. Neither personal nor overhead data are exchanged unless explicitly authorized.
All sensible data (such as personal data, system configurations, known vulnerabilities with their locations) are encrypted if they must be transmitted over unsecured environment as stated below.

- # Communication and authentication

In view of the types of information that MIL.CERT-UA deals with, emails, telephone and Signal will be considered sufficiently secure to be used. Unencrypted e-mail will not be considered particularly secure, but will be sufficient for the transmission of low-sensitivity data.
If it is necessary to send highly sensitive data by e-mail, encryption (preferrably PGP) will be used. Network file transfers will be considered to be similar to e-mail for these purposes: sensitive data should be encrypted for transmission.
All e-mail or data communication originating from MIL.CERT-UA will be digitally signed, using the generic PGP key mentioned above, or the MIL.CERT-UA.

- # Incident response

MIL.CERT-UA will assist system administrators in handling the technical and organizational aspects of incidents. In particular, it will provide assistance or advice with respect to the following aspects of incidents management:

Incident triage
- Investigating whether indeed an incident occurred.
- Determining the extent of the incident.

Incident coordination
- Determining the initial cause of the incident (e.g. vulnerability exploited, …).
- Facilitating contact with other sites which may be involved.
- Facilitating contact with appropriate law enforcement officials, if necessary.
- Making reports to other CERTs.
- Composing announcements to users, if applicable.
- Ensuring adequate threat sharing information for proactive measures.

Incident resolution
- Helping to remove the vulnerability.
- Helping to secure the system from the effects of the incident.

- Collecting evidence of the incident.

In addition, MIL.CERT-UA will collect statistics concerning incidents processed, and will notify the community as necessary to assist it in protecting against known attacks.

• Proactive services

MIL.CERT-UA coordinates and maintains the following services to the extent possible depending on its resources:

- list of security contacts
- security recommendations
- training and educational services
- vulnerability notification & assistance

• Disclaimer

While every precaution will be taken in the preparation of information, notifications and alerts, MIL.CERT-UA assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.