NCSC CVE Assignment Policy

Guidance on vulnerabilities eligible for CVE assignment by the NCSC.

Purpose

The NCSC is a Vulnerability Coordinator CVE Numbering Authority (CNA) within the CVE Program. Our role is to act as a trusted third-party coordinator for vulnerabilities discovered in other entities' products within our specific geographic and sector scope.

This policy explains the circumstances in which the NCSC may assign CVE Identifiers and publish corresponding CVE Records.

The NCSC operates within a scope approved through the CVE Program and follows the current CVE Program policies, CNA Operational Rules and Terms of Use. CNA status allows the NCSC to assign identifiers; it does not mean that the NCSC endorses a product, certifies the severity of a vulnerability, or guarantees that a vulnerability has been fixed.

What is a vulnerability?

The NCSC applies the CVE Program definition of vulnerability:

An instance of one or more weaknesses in a Product that can be exploited, causing a negative impact to confidentiality, integrity, or availability; a set of conditions or behaviors that allows the violation of an explicit or implicit security policy.

NCSC assignment scope

The NCSC may assign a CVE ID where all of the following apply:

- The vulnerability affects an industrial control system (ICS) or operational technology (OT) product.
- The affected product is developed or maintained by a UK-based company.
- The vulnerability is reported to, identified by, researched by or coordinated by the NCSC.
- The NCSC has reasonable evidence that a CVE-eligible vulnerability exists.
- The vulnerability has been, or is expected to be, publicly disclosed.
- No CNA with more appropriate scope is handling the assignment, or the case has been referred or escalated to the NCSC in accordance with CVE Program processes.

The NCSC will not assign a CVE ID outside of the above scope. Where another CNA has more appropriate scope, the NCSC will refer the request or coordinate with that CNA.

Requesting a CVE ID

Requests should be sent to security@ncsc.gov.uk.

Reports containing non-public or sensitive technical information should be encrypted using the NCSC PGP key detailed in our security.txt.

Where available, please provide:

- Reporter name and contact details.
- Supplier and product name.

- Affected versions and components.
- A technical description of the weakness and security impact.
- Reproduction steps, proof-of-concept material, or other supporting evidence.
- Known attack prerequisites or required privileges.
- Information about any observed exploitation.
- Fix or mitigation information, if available.
- Whether the supplier has been contacted and its response.
- Whether a CVE ID has already been assigned or requested from another CNA.
- Whether the issue has already been publicly disclosed.
- Relevant advisory or public reference links.
- The proposed disclosure date.
- Any credit or acknowledgement preferences.

Please do not include personal data, credentials, live secrets, or unrelated sensitive information unless it is necessary to assess the report.

What happens after a request?

The NCSC will acknowledge receipt within 10 working days. An acknowledgement does not mean that the report has been accepted as a vulnerability or that a CVE ID will be assigned.

The NCSC may:

- Request further information.
- Accept the case for coordination.
- Reserve or assign a CVE ID.
- Coordinate with the supplier or another CNA.
- Refer the requester to the CNA with a more appropriate scope.
- Explain that the report is outside the NCSC's scope or does not currently provide sufficient evidence for assignment.

The NCSC will make reasonable, good-faith efforts to notify and coordinate with the supplier. If the NCSC assigns a CVE ID, we will provide the identifier to the reporter.

Publication

Reservation or assignment of a CVE ID does not by itself make the vulnerability public.

The NCSC will aim to publish the CVE Record at the time of coordinated public disclosure and will comply with applicable CVE Program publication deadlines.

CVE Records may subsequently be corrected, updated, merged, split, marked as disputed or rejected where appropriate under CVE Program processes.

Further information

- CVE Program
- CVE Program Glossary
- CNA Operational Rules
- NCSC Security.txt

- NCSC Vulnerability Management Guidance

PUBLISHED

17 November 2026

WRITTEN FOR

Cyber security professionals

Large organisations

Public sector