NCSC Scanning information

This page provides information on the NCSC's scanning activities. You may have been referred here by information left by one of our scanning probes if a system you own or administer has been scanned.

Why is the NCSC carrying out scanning activities?

As part of the NCSC's mission to make the UK the safest place to live and do business online, we are building a data-driven view of "the vulnerability of the UK". This directly supports the UK Government Cyber Security Strategy relating to Understanding UK Cyber risk (Objective 1) . This will help us to:

- better understand the vulnerability and security of the UK
- help system owners understand their security posture on a day-to-day basis
- respond to shocks (like a widely exploited zero-day vulnerability)

How does the NCSC determine which systems to scan?

These activities cover any internet-accessible system that is hosted within the UK and vulnerabilities that are common or particularly important due to their high impact. The NCSC uses the data we have collected to create an overview of the UK's exposure to vulnerabilities following their disclosure, and track their remediation over time.

How is scanning performed?

To identify whether a vulnerability exists on a system, we first need to identify the existence of specific associated protocols or services. We do this by interacting with the system in much the same way a web browser or other network client typically would and then analysing the response that is received.

For example, we may be able to determine the existence of a vulnerability known to exist in version ***X*** of a type of commonly used web server software by making a web request to the URL ".../login.html" and detecting the value "version X" in the content of the page that is returned. If the vulnerability is then remediated in a subsequent version ***Y***, we can identify this by similarly detecting the value "version Y" in the response.

By repeating these requests on a regular basis we maintain an up-to-date picture of vulnerabilities across the whole of the UK.

What information does the NCSC collect and store?

We collect and store any data that a service returns in response to a request. For web servers, this includes the full HTTP response (including headers) to a valid HTTP request. For other services, this includes data that is sent by the server immediately after a connection has been established or a valid protocol handshake has been completed. We also record other useful information for each request and response, such as the time and date of the request and the IP addresses of the source and destination endpoints.

We design our requests to collect the smallest amount of technical information required to validate the presence/version and/or vulnerability of a piece of software. We also design requests to limit the amount of personal data within the response. In the unlikely event that we do discover information that is personal or otherwise sensitive, we take steps to remove the data and prevent it from being captured again in the future.

How can I attribute activity on my systems to NCSC Scanning?

All activity is performed on a schedule using standard and freely available network tools running within a dedicated cloud-hosted environment. All connections are made using one of two IP addresses:

- 18.171.7.246
- 35.177.10.231

Note that these IP addresses are also both assigned to **scanner.scanning.service.ncsc.gov.uk** with both forward and reverse DNS records. Scan probes will also attempt to identify themselves as having originated from NCSC where possible, for example by including the following header within all HTTP requests:

X-NCSC-Scan: NCSC Scanning agent - https://www.ncsc.gov.uk/scanning-information

---

What precautions and safety measures does the NCSC take when scanning?

The NCSC is committed to conducting scanning activities in a safe and responsible manner. As such, all our probes are verified by a senior technical professional and tested in our own environment before use. We also limit how often we run scans to ensure we don't risk disrupting the normal operation of systems.

Can I opt-out of having servers that I own or maintain being scanned?

Yes. Please contact scanning@ncsc.gov.uk with a list of IP addresses that you wish to exclude from any future scan activity and we will endeavour to remove them as soon as possible once validated.

Who can I contact for any other questions or queries I may have?

Please complete the form on the General Enquiries section of our website and we will endeavour to respond to you as soon as possible.

PUBLISHED

1 November 2022

REVIEWED

1 November 2022

WRITTEN FOR

Public sector

Large organisations

Cyber security professionals

Small & medium sized organisations