CE Plus
Client Guide

Date: January 2022

CE+ Pre-Assessment Briefing

Before you begin on your CE+ assessment, here is a brief explanation of the general prerequisites for testing. We will need the following prerequisites for tests:

- to be able to send arbitrary emails to an account operated by the Applicant — that is, an external email system that performs no filtering and is not deny listed
- users with appropriate credentials to perform the tests · working email clients (and associated email addresses) and web browsers on a sample of the end user devices in scope

Test 1: Remote vulnerability assessment

To test whether an Internet-based opportunist attacker can hack into the Applicant's system with typical low-skill methods.

Prerequisites

You will need:

- a vulnerability scanning tool that has been approved by the Assessors
- to have identified the IP addresses to be scanned Where dynamic IP addresses are in use for an Internet connection, the scope may be defined in terms of appropriate DNS entries.

What devices are tested

All end user devices within the sample set.

What we are testing for

The following tests apply to all computing devices within the boundary of scope. This includes:

- end user devices (EUDs) that can connect to organisational data or services
- servers on which standard (that is, non-administrator) users can obtain an interactive desktop environment
- all types of cloud service (IaaS, Paas, or SaaS)

On all but the smallest networks it will be impractical to test every device that is within the agreed boundary of scope. Instead, we test a representative sample

All cloud services must be tested using a representative sample of user accounts. This must consist of at least one normal user and one administrative user for every cloud service used. The same users can be used across multiple cloud services. We are testing to ensure that there are no vulnerabilities rated as High Risk or Critical Risk, or that have a CVSS v3 score of 7.0 or higher.

Test 2: Check patching, by authenticated vulnerability scan of devices

This test is performed on a sample set of EUD, servers and IaaS instances.

The purpose of this test is to identify missing patches and security updates that leave vulnerabilities that threats within the scope of the scheme could easily exploit.

Prerequisites

In addition to the general prerequisites testing, you will need:

- a vulnerability scanning tool that has been approved by the Assessor
- Each device to be tested, scan with the approved vulnerability scanning tool

What devices are tested

All end user devices within the sample set.

What we are testing for

We are testing to ensure that there are no missing patches or service packs and that there are no vulnerabilities with a High Risk or Critical Risk rating and that there are no risks with a CVSS v3 score of 7.0 or higher.

Test 3 Check malware protection

This test is performed on sampled EUD, servers and IaaS instances to check that all the devices in scope benefit from at least a basic level of malware protection.

We need to identify what type of malware protection each device in the sample set uses: antivirus software, application allow listing or application sandboxing.

What devices are tested

All end user devices within the sample set.

What we are testing for

We will be manually checking each machine within the sample set of machines to ensure that:

- all anti-malware definitions released within the 24 hours prior to testing have been installed
- all anti-malware engine updates released within the 30 days prior to testing have been installed

Test 4 Check effectiveness of defences against malware delivered by email

This test is performed on any sampled EUD, servers and cloud environments where email can be received by users (“user environments”).

What devices are tested

All end user devices within the sample set.

What we are testing for

We are manually testing to test the protection against malware that is delivered via email attachments. For each user environment in the sample set, we will need to:

1. Establish a baseline by sending a simple email from your remote test account, with no attachments.
2. Attempt to send each test email from your remote test account to the test destination and observe the user attempting to open each attached test file.

Test 5 Check defences against malware delivered through a website

This test is performed on any sampled EUD, servers and cloud environments where browsing can be performed by users (“user environments”). We will instruct the user to browse to a specific URL (https://ce-plus.hedgehog.gi/testfiles) and download each of the files and attempt to open them.

What devices are tested

All end user devices within the sample set.

What we are testing for

This tests whether user environments have protection from malware delivered through a website. We are specifically looking to see if the download is blocked or if the user can download the files, can they execute them. A failure is issued if any of the files can be executed without a warning.

Test 6 Check Multi-factor authentication configuration

This test is performed test on all cloud services. to test cloud services declared in scope have been configured for multi factor authentication (MFA). Users of sampled devices to attempt to log into the organisations cloud services using their organisation issued accounts.

What is tested

All cloud services listed in the CE questionnaire.

What we are testing for

All cloud services are to be tested for User and Administrator Access. Where multiple cloud services share an authentication service this test only needs to be performed once for each authentication service. We are testing to observe that multi-factor authentication is in place for cloud environments.

Test 7 Check account separation

This test is performed on any of the sampled end user devices, servers and cloud environments where administrative processes can run. The purpose is to test user accounts don't have administrator privileges assigned.

What is tested

All sampled devices need to be tested.

What we are testing for

When logged in with a standard user account, they attempt to run a defined administrative process. A failure will be issued is a standard user profile is able to run an administrative process.