ncc group

Source Code Review

In a source code review, NCC Group's team of consultants will examine your code both for common vulnerabilities, such as debug code left in the production version or buffer overflows, and subtler problems such as error logs revealing details about your code's internal workings.

All software, no matter how well-written, has bugs. These bugs can, if an attacker becomes aware of them, become a vector for attack. It is difficult for even the most skilled programmers to see the flaws in their own work, and an outside review of the
code will often turn up potentially-dangerous vulnerabilities that have been missed by the development team.

With a source code review from NCC Group, you can minimise the number of vulnerabilities in your software, and gain the assurance you need that your source code keeps to best security practices.

What we do

Everysourcecodereview is different, but typically a review will include:

Memory management:
The code will be examined for issues such as buffer overflows, heap overflows, double-frees and use-after-frees, all of which can potentially lead to remote code execution vulnerabilities. This could allow an attacker to gain control of the machine on which the application is running.

Build configuration:
NCC Group can review the build configuration for the software to ensure that advantage is taken of anti-reverse engineering features offered by the compiler and operating system. At this stage we may discover flaws that would allow an attacker to reverse- engineer the code.

Trust boundary:
Code which implements key trust boundary functions such as encryption, login, or input validation and filtering is examined in detail. All code which handles data originating from untrusted sources, such as
input files or network traffic, will be targeted. At this stage, we might discover vulnerabilities such as SQL injection and cross-site scripting susceptibility.

Error handling:
There are instances where error conditions occur during normal operations and are not handled properly. If an attacker can identify the errors that the web service fails to handle correctly, they can systematically force those errors, revealing system information.

Flaws we look for include:

Privilege escalation:
Forcode which runs at a high privilege level, such as services or drivers, the processing of user-supplied data is checked in order to find any privilege escalation bugs.

Sensitive information hardcoded:
We attempt to identify sensitive information such as encryption keys, hard-coded backend credentials, server IP addresses, or default credentials which should not be present in the application but frequently remain due to developer oversight. An attacker may be able to find these by reverse engineering the application.

Device storage:
If the code assessed is for a mobile application, it is important to identify all application data which is being stored locally on the device (either in databases or on the file system), ensuring that all sensitive data is encrypted. We will assess the application's interaction with local storage, looking for unprotected secrets written to local storage which can be read by malicious users, or files which can be manipulated to subvert the application.

For more information from NCC Group on our G-Cloud 15 service, please contact:

+44 (0)161 209 5200

bidteam@nccgroup.com