CIBERSECURITY

Express Security Assessment

WOULD YOU LIKE TO HAVE AN UP-TO-DATE INSIGHT OF THE RISK ASSOCIATED WITH YOUR REMOTE ACCESS SYSTEMS IN 5 DAYS?

Due to the situation caused by COVID-19, many companies are facing the need to provide their employees with remote access, in order to guarantee operational continuity.

There is a risk that this contingency deployment may introduce vulnerabilities in remote access systems. This particularly applies to VPN systems and virtual desktops (VDI).

Our aim is to provide those responsible for security with a RAPID SECURITY ASSESSMENT for their remote access systems, focussing on the identification of the most relevant vulnerabilities.

FAST, RELIABLE AND COST EFFECTIVE

marketing.TIC@gmv.com

gmv.com

gmv®
INNOVATING SOLUTIONS

The focus of the assessment is remote access systems:

- **VPN terminators**
  For the assessment of VPN terminators, the role of a malicious external agent attempting to gain unauthorised access is adopted.

- **Virtual desktop infrastructure (VDI)**
  In the case of VDI, the role of an authorised user is adopted, and the privilege level is evaluated.

DELIVERABLES

INTERMEDIATE DIAGNOSTICS (EXCEL FORMAT).

FINAL DIAGNOSTICS (PDF FORMAT).

CRITICAL VULNERABILITY ALERTS

DISCOVERY

Port discovery and scanning.
Infrastructure analysis.

VPN DIAGNOSTICS

Loginbypass testing based on VPN protocol (PPTP, L2TP, Ipsec/IKE, SSL, etc.).
Validation of password quality.
Testing of access alternatives.
Encryption testing.

VDI DIAGNOSTICS

Bypass testing of security restrictions (cmd console, powershell, etc.).
Testing with file writing techniques.
Data extraction testing.

THIRD PARTY VULNERABILITY DIAGNOSTICS

To check for possible known vulnerabilities associated with the VPN/VDI software.
To also check known vulnerabilities in the underlying infrastructure software.

Service process

INFORMATION GATHERING

The service begins with the gathering of information on the terminators supplied via the use of OSINT techniques.

1

EXPLORATION

The service continues with an analysis of the underlying infrastructure of the VPN and the VDI.

2

FINGERPRINTING

Information is actively obtained on the technologies used, so that the auditors can define the testing to be carried out during subsequent stages, and how to check whether there are known vulnerabilities to be tested for.

3

AUTOMATED SCANNING

Automated scanning of the VPN terminators or the VID infrastructure open to the internet is carried out, in order to determine any possible “low-hanging fruit” which an attacker may take advantage of.

4

MANUAL CHECKING

Manual checking provides confirmation that the vulnerabilities found during the previous stage are not false positives. Furthermore, testing is carried out to detect those vulnerabilities that automatic analysis does not detect.

5

REPORT

The auditors produce two reports: a progress report half way through the process in order to deal more rapidly with possible vulnerabilities detected, and a final report including the vulnerabilities and the solutions recommended by GMV.