CVSS BASE SCORE FOR SOCIAL ENGINEERING

Exploitability Metrics

•Attack Vector - The vulnerability can be remotely exploited over the Internet.

•Attack Complexity - There are no specific pre-conditions required for exploitation.

•Privileges Required - No privileges or special access are required.

•User Interaction - A user must complete some steps for the exploit to succeed.

Impact Metrics

•Confidentiality - The attacker has full access to all resources in the impacted system.

•Integrity - The attacker can modify any/all information on the target system.

•Availability - There is a complete loss of availability of the impacted system or information.

Scope

•Scope : - An exploited vulnerability can have a carry-over impact on another system.

Using the CVSS calculator

CVSS BASE SCORE FORMULA:

ROUNDUP(((0.6 * IMPACT) + (0.4 * EXPLOITABILITY) + (0.1 * SCOPE)) * F(IMPACT))

we can calculate the CVSS base score as follows:

Exploitability Score: 3.9

Impact Score Formula:

Impact = 10.41 * (1 - (1 - C) * (1 - I) * (1 - A))

Impact Score: 5.9

Scope = 1.0 if S is Changed, otherwise Scope = 0.0

Scope Score: 1.0

CVSS Base Score: 8.6 (based on Exploitability Score, Impact Score, and Scope Score)

So, the CVSS base score for a Social Engineering vulnerability is 8.6, which is considered a High severity vulnerability.

Here is the breakdown of the scores:

- Exploitability Score: 3.9
- Impact Score: 5.9
- Scope Score: 1.0
- CVSS Base Score: 8.6