SEVERITY LEVELS - MONITORING

CRITICAL

Emergency Situation – Active Cyber Attack

Evidence of an attacker operating from an escalated account (i.e. admin), malware or attack behavior on a high value host ie Domain Controller. Multiple machines displaying attack behavior, data exfiltration. Poses imminent or critical threat to the infrastructure or organisation.

SEVERE

Immediate functional impact

Successful unauthorized logins, manual malicious commands being run on a host signifying an active persistent threat, multiple machines displaying similar attack evidence. Likely to result in significant impact to the organisation.

HIGH

High Possibility of Functional Impact

Credential loss due to phishing, verified malware execution on one or more hosts, detection of unauthorized program tasks or user activities. Likely to result in demonstrable impact to the organisation.

MEDIUM

Moderate Possibility of Functional Impact

Malware quarantined or blocked, suspicious email(s) quarantined, suspicious inbound/outbound connections blocked, evidence of suspicious sign-in attempts/failures. May impact the organisation.

LOW

Slight possibility of functional impact

Vulnerable services discovered or security risks. Unlikely to immediately impact the organisation.

RISK LEVELS - VAPT

Based on the approach described above, there are 5 levels. When assessing the issues found, the following categories were used to indicate the impact:

LEVEL 5 : CRITICAL RISK

The Critical level is used for issues that:

- give an attacker complete control over a system from a remote location
- give an attacker full access to (business) critical data
- damages the availability after the attack permanently without any conditions

Characteristics of issues at this level are:

- an attacker does not need any (special) rights to carry out the attack
- an attacker does not need (specific) knowledge of the system or users
- an attacker does not have to convince users (for example by social engineering) to act for the attack to succeed
- exploits and tooling are publicly available

Issues at this level can be automatically exploited by, for example, worms and tooling. Examples of such issues are attacks that can be used to remotely execute code on the system, SQL injection and persistent cross-site scripting attacks that do not require authentication and Denial of Service attacks with a lasting effect.

LEVEL 4 : HIGH RISK

Issues in the High category are problems that:

- give an attacker complete control over a system from a remote location
- give an attacker full access to (business) critical data
- damages the availability after the attack permanently, but require one of the following conditions must be met:
    - an attacker needs (special) rights to perform the attack (e.g. an account or access to the internal network)
    - an attacker needs specific knowledge of the system or users (for example, a non-standard configuration or knowledge of an application)
    - an attacker must convince a user (for example, through social engineering) to act for the attack to succeed
    - exploits and tooling are not publicly available and have to be developed by the attacker

Issues at this level can be exploited in a targeted attack on employees or by (internal) users who have specific knowledge of the system. Examples are the ability to access administrator functionalities as a standard user (vertical privilege escalation), SQL injection and persistent cross-site scripting where authentication is required, being able to access company or system-critical information that should not normally be accessible to the user and Denial of Service attacks with lasting effect that can only be executed from the internal network.

LEVEL 3 : MEDIUM RISK

Issues in the Medium category are problems that:

- only give an attacker control over a system
- only give an attacker partial access to (business) critical data
- it only affects availability during an attack and for which one of the following conditions must be met:
    - an attacker needs (special) rights to perform the attack (eg an account or access to the internal network)
    - an attacker needs specific knowledge of the system or users (for example, a non-standard configuration or knowledge of an application)
    - an attacker must convince a user (for example, through social engineering) to take action for the attacker
    - exploits and tooling are not publicly available

Issues at this level can be exploited in a targeted attack on employees or by (internal) users who have specific knowledge of the system. Examples are being able to access functionalities of other users (horizontal privilege escalation), reflected cross-site scripting attacks or partially accessing business or system-critical information that should normally not be accessible to the user.

LEVEL 2 : LOW RISK

Issues in the Low category are problems that are very difficult to abuse or where the effects have a low impact on the system or business. Examples are attacks that can only be executed if an attacker has direct access to a system or attacks that have minimal impact on availability during an attack.

LEVEL 1 : INFORMATIONAL

The Informative level is used for issues that cannot be directly exploited but can help an attacker to plan or execute a follow-up.

In addition, a sixth category is used in the report:

LEVEL 0 : POSITIVE

This level is used for findings during the test that actively prevented an attempt and thus make a positive contribution to the overall safety of the system.