Setting up a pen test for your system

Cybersecurity is unique for every system. It is a symphony consisting of many different instruments that all need to be tuned to perfection. Of course, we have done a pen test for Barco CTRL itself (contact us if you want to know more about the results), but this is only for our system in a closed environment. To assess the cybersecurity of a complete infrastructure, the pen test should be conducted on the actual live environment. In this article, we describe the different things to consider when performing such a test in your organization.

What is a CVSS score?

The CVSS score stands for Common Vulnerability Scoring System, which is a standard way of assessing the severity of computer system vulnerabilities. It's like a numerical rating system that helps organizations prioritize and respond to security issues. The score considers various factors such as the ease of exploitation, potential impact on confidentiality, integrity, and availability of the system, and whether there are any mitigating factors or workarounds available.

Scores typically range from 0 to 10, with 10 being the most severe. The higher the score, the more critical the vulnerability is considered. This scoring system provides a common language for security professionals to communicate about the severity of vulnerabilities and helps organizations make informed decisions about how to allocate resources for patching and mitigating risks.

How to determine the CVSS

The CVSS provides a structured method for assessing the severity of vulnerabilities in computer systems. The score is calculated based on several metrics that evaluate the characteristics and potential impact of the vulnerability.

1. Base Score

This score reflects the intrinsic qualities of the vulnerability and is calculated using several metrics:

- **Attack Vector (AV):** Describes what kind of access an attacker needs to the system before they can exploit the vulnerability. Options are, in order of decreasing difficulty to exploit and issue, physical access (P), local access (L, e.g. being logged into the system), access from an adjacent network (A), or access via the network (N) – possibly across several networks**.**
- **Attack Complexity (AC):** Considers how complex the attack is to execute, with options like low (L) or high (H).
- **Privileges Required (PR):** Evaluates the level of privileges an attacker needs to exploit the vulnerability, ranging from none (N), general user privileges (L) to having administrative privileges (H).
- **User Interaction (UI):** Considers whether user interaction is required to exploit the vulnerability, such as none (N) or required (R).
- **Scope (S):** Reflects the extent of impact beyond the vulnerable component, with possible values of unchanged (U) or changed (C).

2. Temporal Score

This score considers factors that may change over time, such as exploit availability, remediation level, and report confidence.

3. Environmental Score

This score takes into account the impact of the vulnerability on a specific environment, such as the importance of the affected system, its need for protection of confidentiality, integrity and availability, and the security controls in place.

These scores are combined using a specific formula to produce the overall CVSS score. The resulting score is a numeric value between 0.0 and 10.0, where higher scores indicate greater severity.

CVSS provides a standardized and objective way to prioritize vulnerabilities, enabling organizations to allocate resources efficiently for patching and mitigation efforts. However, it's essential to interpret the score in the context of the organization's unique environment and risk tolerance.

How do you "scope" a pen test

Cyber threats are constantly evolving, and new vulnerabilities emerge regularly. As we highlighted before, regular pen testing helps organizations stay ahead of these threats by continuously assessing and improving their security posture. By discovering these weaknesses before attackers do, organizations can address and fix them proactively.

Device Scope

Barco welcomes customers to engage in cybersecurity penetration tests of our product. While customers can design the test to their particular use case, we thought this would benefit customers new to scoping pen tests.

In some recent reports, we saw that end customers had been paying for tests that included results from equipment that isn't Barco. This makes sense if planned as a complete test of the final system in which Barco is only a part. Still, we wanted to highlight which devices are not Barco CTRL and which are, so other customers can direct the security professionals' efforts accordingly.

Devices that are not part of the Barco CTRL scope are:

- **Network switches.**
- **Devices providing the network services (Gateway, DNS, NTP, DHCP, IdP etc).**
- **Source machines or devices such as Cameras.**
- **Computers or Laptops that are used for accessing the system.**
- **Screens or monitors connected to the decoder.**

Barco might provide some of the above devices for a temporary demo, but they are not part of our product offering. Any vulnerabilities should be reported to the equipment manufacturers and not to Barco. Please note that other manufacturers' equipment is not covered under the Barco responsible disclosure policy (https://www.barco.com/en/about/trust-center/responsible-disclosure).

Test Scope

We have broken the test into various sections, as they approach different parts of the product and involve different skill sets on the testing side.

1. Simulation of attack against all three devices

Simulation of attacks against all three devices (Encoder – NGS-D440, Decoder – SAN-050 and Server – SAS-050) from the perspective of an attacker having physical access (stopping short of opening the enclosure if the customer wishes to have the devices still covered under the warranty/support contract). Prove that:

- Exposed physical ports cannot be used to tamper with the bootstrap process of the devices (for example, to boot into a rogue firmware and backdoor the device or extract Barco certificate)
- Standard USB-adapters cannot be used to increase attack surface of the devices (USB network adapters do not allow local firewall bypass, USB serial adapter do not expose system console, USB keyboard cannot be used to log into the system and send commands, ...).

2. Security tests against the operator interface in "Desk" case

The objectives are to make sure that:

- It is not possible to gain unauthorized access to the underlying OS of the decoder via keyboard/mouse/screen connected to the decoder by tampering with the decoder during the bootstrap process
- It is not possible to bypass Desk login prompt and gain access to the UI
- It is not possible to gain unauthorized access to the underlying OS of the decoder via keyboard/mouse/screen connected to the decoder once a user or admin is logged into the desk

3. Security tests against the "wall" case.

The objectives are to make sure that:

- It is not possible to gain unauthorized access to the underlying OS of the decoder via keyboard/mouse/screen connected to the decoder by tampering with the decoder during the bootstrap process,
- It is not possible to gain unauthorized access to the underlying OS of the decoder via keyboard/mouse/screen connected to the decoder once loaded

4. Network vulnerability scan of all devices

The objectives are to make sure that:

- The exposure is strictly limited to minimum required network services
- The exposed services enforce strong encryption and authentication

5. Security test of SAS web admin UI

This is done following OWASP Web Security Testing Guide (WSTG) methodology. The test should cover at least the OWASP Top 10.

The objectives of the test include but are not limited to:

- Local and external (LDAP) authentication providers prevent unauthorized access the webadmin UI, ,
- Even an authenticated administrator user cannot escalate privileges and gain privileged access to the underlying OS (including abuse of software update process).

6. Security test of the REST APIs

'Configure and operate tests', provided by SAS following OWASP WSTG.

7. Security test of device provisioning and configuration process

The objectives are to ensure that:

- mTLS protects the confidentiality and integrity of all flows between all devices (SAS, decoder, encoder) during the provisioning process and prevents the admission of untrusted devices.

8. Security test - traditional AV / USB-HID source use case.

The objectives are to ensure that:

- Integrity and confidentiality of SRTP/RTSPS/VNC flows are protected by mTLS

Contact us for further information

Existing partners and end users with a mutual NDA can contact their sales team members to receive a copy of our latest pen test results.

We are actively working towards a “trust package” that will be publicly available, and that will include our latest pen test and other important information for all the cyber security stakeholders. More information will be available as we get further down this process.