Main website Vulnerabilities report

And how to prevent it.

1) Common Platform Enumeration (CPE) is a structured naming scheme for information technology systems, software, and packages. It includes a formal name format, a method for checking names against a system, and a description format for binding text and tests to a name.

- Regarding vulnerabilities in CPE, it is important to note that CPE itself is not vulnerable. However, vulnerabilities can be associated with CPE names. The National Vulnerability Database (NVD) provides an official CPE dictionary that lists all official CPE names.

- **To stop vulnerabilities** associated with CPE names, it is important to keep the software up-to-date with the latest patches and security updates. Additionally, it is important to use security tools such as firewalls and antivirus software to protect against potential attacks.

2) **Device Type** vulnerabilities are a type of security vulnerability that can be exploited by attackers to gain unauthorized access to a device or network. To prevent such vulnerabilities, it is important to follow some best practices:

- **Use strong passwords**: Use strong passwords that are difficult to guess and avoid using the same password for multiple accounts.
- **Use two-factor authentication**: Two-factor authentication adds an extra layer of security to your accounts by requiring a second form of authentication, such as a code sent to your phone.
- **Use firewalls and antivirus software**: Firewalls and antivirus software can help protect against potential attacks by blocking malicious traffic and detecting and removing malware.
- **Limit access to sensitive data**: Limit access to sensitive data by using role-based access control (RBAC) and other access control mechanisms.
- **Implement intrusion prevention systems (IPS)**: IPS can help detect and prevent attacks by monitoring network traffic for signs of malicious activity.

3) HTTP Server Type and Version vulnerabilities can be exploited by attackers to gain unauthorized access to a device or network. To prevent such vulnerabilities, it is important to follow some best practices:

- **Limit the information that your web server presents**: You can limit the information that your web server presents by creating/editing the following directives in httpd.conf: ServerTokens Prod. This will configure Apache to not

send any version numbers in the server response header so that the server line will be: Server: Apache.

- **Use security tools**: Security tools such as packet-layer firewalls and web application firewalls can block non-typical HTTP options to help minimize the risk to the environment. Removing or denying those HTTP options with a configuration management program can also reduce the risk to the web platform.
- **Implement intrusion prevention systems (IPS)**: IPS can help detect and prevent attacks by monitoring network traffic for signs of malicious activity.
- **Use secure HTTP headers**: Use secure HTTP headers such as X-Content-Type-Options, X-XSS-Protection, X-Frame-Options, and Content-Security-Policy to protect against potential attacks.

4) Fully Qualified Domain Name (FQDN) Resolution vulnerabilities can be exploited by attackers to gain unauthorized access to a device or network. To prevent such vulnerabilities, it is important to follow some best practices:

- **Remove dangling DNS entries**: Dangling DNS entries are DNS records that point to a deprovisioned resource. These entries can be exploited by attackers to redirect traffic intended for an organization's domain to a site performing malicious activity. To prevent this, it is important to remove any dangling DNS entries.
- **Use FQDN filtering in network rules**: You can use Fully Qualified Domain Name (FQDN) filtering in network rules based on DNS resolution in Azure Firewall and Firewall policy. This capability allows you to filter outbound traffic with any TCP/UDP protocol (including NTP, SSH, RDP, and more).
- **Perform regular security audits**: Regularly perform security audits to identify vulnerabilities in your systems and networks.
- **Use secure HTTP headers**: Use secure HTTP headers such as X-Content-Type-Options, X-XSS-Protection, X-Frame-Options, and Content-Security-Policy to protect against potential attacks.
- **Limit access to sensitive data**: Limit access to sensitive data by using role-based access control (RBAC) and other access control mechanisms.

5) OS Identification vulnerabilities can be exploited by attackers to gain unauthorized access to a device or network. To prevent such vulnerabilities, it is important to follow some best practices:

- **Keep your software up-to-date**: Regularly update your software with the latest patches and security updates. This will help to fix any known vulnerabilities in the software.
- **Use strong passwords**: Use strong passwords that are difficult to guess and avoid using the same password for multiple accounts.

- **Use two-factor authentication**: Two-factor authentication adds an extra layer of security to your accounts by requiring a second form of authentication, such as a code sent to your phone.
- **Use firewalls and antivirus software**: Firewalls and antivirus software can help protect against potential attacks by blocking malicious traffic and detecting and removing malware.
- **Limit access to sensitive data**: Limit access to sensitive data by using role-based access control (RBAC) and other access control mechanisms.