ManageEngine
Network Configuration Manager

TOP 4 BEST PRACTICES TO EFFECTIVELY SAFEGUARD NETWORK DEVICES' FIRMWARE FROM VULNERABILITIES

Nikhil Frederick J

Introduction

As networks become more and more complex, so does the daunting task of managing security for the network devices present in one's infrastructure. Security risk is a common factor, and devices' firmware is a common target for data hackers.

Since firmware is considered critical for device workflow and operations, a successful attack on it is no ordinary security threat. If the firmware attack is severe, the attacker may gain access to all device details and gain a strong foothold in the entire network infrastructure. Also, network infrastructures containing thousands of devices become a soft target if not handled with utmost care.

According to **Microsoft's March 2021 Security Signals study**, more than 80% of enterprises have experienced at least one firmware attack in the past two years, but only 29% of security budgets are allocated to protect firmware.

This e-book will give you clear insights on how you can effectively manage firmware vulnerabilities using Network Configuration Manager, and eradicate external threats completely by putting up an unbreachable barrier.

1. Conduct regular scans, both internal and external

Regular scanning—that is, daily—of network devices will provide clear insights into various device details, such as its operation state, its points of weakness, and how vulnerable it is to external threats.

External scanning takes the perspective of an external threat and determines how it will affect devices by targeting IP addresses, firewalls, open ports, etc. Internal scanning

looks within to see where a threat breached the network, and how to avoid it from further exploiting the environment. Both these scans will give a clear picture of the devices' firmware, and users can easily apply necessary fixes if anything is out of place.

This process may not always be manual. If you have network software that supports automation, this process can be automated, and the scan results will provide the insights. This is beneficial for large enterprises handling thousands of devices.

Facts

According to **IBM's 2022 Cost of a Data Breach report,** for the 12th year in a row, the United States holds the title for the highest cost of a data breach at USD 9.44 million, which is USD 5.09 million more than the global average.

2. Practice good inventory and asset management

A separate inventory containing devices that are weak or have been affected by a vulnerability is a must. In a large network environment, it can be difficult for admins to keep track of all the devices' firmware health and if they have been affected in one way or another. This will eventually lead to a device being in a highly vulnerable state and attacked, potentially bringing down the entire network in the long run.

Therefore, a good automated firmware inventory management tool that will list the affected devices and users and can apply patch fixes accordingly is necessary. A severity index should also be present along with the inventory list so users can take action and fix higher severity, vulnerable devices first. Providing important insights about the vulnerability along with patch fixes is an important addition to your armory, enabling users to learn how the vulnerability works and take remediation to next level. This will help keep your devices safe from any type of malicious threats, and also provides a bird's-eye view of all known vulnerabilities.

Facts

According to a **blog by Quantum Technologies** in 2021, firmware attacks have increased by 5x over the last four years, and 83% of businesses have experienced a firmware attack in the last two years.

3. Have knowledge on common areas of weakness causing prominent firmware attacks

There are certain core firewalls and routers in an enterprise's network. And since a firewall is your first line of defense from external threats, you must perform a clear and thorough inspection of your firewalls at regular intervals and apply the latest compliance rules. It's also critical to regularly check if there are any misconfigured firewalls, which may create an open path for external attacks.

Also, while providing access to firewall configurations, make sure you follow the Zero Trust model and provide least privilege access. Along with this, keep a keen eye on external traffic data exfiltration, since this could be the first sign of a breach incoming.

After firewalls, make sure your core routers are following regulatory standards and working on the safest protocols or encryption standards, such as WPA 2 or WPA 3. This should be standardized for all individuals as well as large enterprises.

Next, keep track of man-in-the-middle attacks since they can lead to decryption of data and credentials that can prove to be costly.

Finally, block network intrusion attacks such as multi-routing, buffer overflows, and protocol impersonation along with DDoS attacks, which cause bad traffic.

Once these are blocked completely from your network and you're performing regular inspections, your network will be at its safest, eventually saving millions of dollars that would otherwise be spent handling malicious attacks.

Facts

According to a study conducted by **Solid State Systems**, 73% of respondents who did not prioritize firmware security experienced a high rate of unknown malware occurrences, whereas 52% of respondents who did prioritize firmware security reported at least one incident of malware-infected firmware infiltrating the company system, which was easily neutralized.

4. Follow best patch management practices for devices

The best fix for firmware vulnerability issues is patches. But if the right patch is not applied, it will be disastrous for the device, and it will still be vulnerable. Therefore, having a clear idea about which patch is suitable for the affected device and its version is advantageous.

The National Institute of Standards and Technology (NIST) has detailed records regarding vulnerabilities, and it also constantly updates with newly found vulnerabilities. The NIST also provides a severity level and and a short description about how each vulnerability acts. It also provides some patch links, but it's always safer to check for patches from the affected vendor; vendors will have the patch links according to versions of the device, enabling you to select a specific device and apply the correct patch.

Facts

According to an **article by Threatpost,** the majority of security teams are more focused on detection and incident response rather than prevention of firmware attacks; only 39% of security teams' time is spent on the latter.

Network Configuration Manager: Your friendly neighborhood network automation and firmware management tool

ManageEngine Network Configuration Manager is a multi-vendor-supporting network configuration and change management (NCCM) tool for managing all your network devices, such as core routers, firewalls, and switches, under one roof.

Network Configuration Manager works best by utilizing five important features in its armory:

- Configuration backups
- Configuration change management
- Automation with script templates called Configlets
- Compliance management
- Firmware vulnerability management

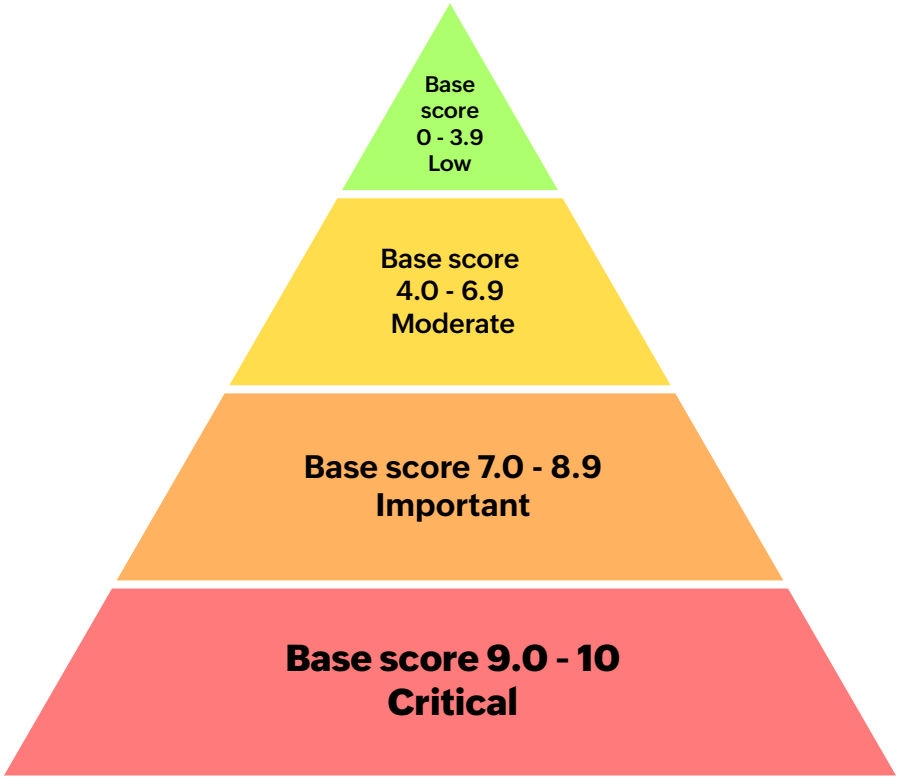
Now, let's look in detail at firmware vulnerability management and how it works in Network Configuration Manager.

In Network Configuration Manager, there is a separate section dedicated to firmware vulnerabilities. Here, details such as CVE ID (vulnerability ID), base score, severity level, the number of devices affected along with with a list of those devices, and various links containing patches are listed. The contents are updated every day and are received from the NIST.

- With Network Configuration Manager, you can view all the vulnerabilities present currently in your network. It also provides an option to view exploits, which displays only the CVE IDs that have info on how one can hack or enter a network, provided by the user who first reported the vulnerability. Such vulnerabilities are severe and have to be prioritized over the rest.

- Sometimes, you may be aware of certain vulnerabilities corresponding to particular vendors, but those vulnerabilities may not be listed in Network Configuration Manager. In that case, you can send us the vendor name, the OS type, and the OS version of the device whose vulnerability has not been listed. Once received, we will automatically fetch and update the vulnerability data for the reported information.
- There is also a search filter provided that helps you display the vulnerabilities associated to the CVE searched. Also, you can filter your search based on severity and exploit availability.
- View the total number of vulnerabilities discovered during a particular period (i.e., the last seven days).
- Network Configuration Manager also provides a device-based vulnerability view, where it lists devices that have a firmware vulnerability along with the number of vulnerabilities in each device.
- Network Configuration Manager also lists all the affected device vendors along with their device versions. Here, the version and the number of vulnerabilities are shown.
- Firmware vulnerability data from the NIST's vulnerability database can be synced with Network Configuration Manager's database. You can schedule a time to sync data on a daily basis. When a scheduled time is set, the synchronization of vulnerability data happens automatically at that time.
- You can also globally search for all vulnerabilities using the vendor name, CVE ID, device OS number, version, or a model. For instance, if you search "Cisco IOS 7000," all the firmware security vulnerabilities present in that particular model will be listed. On further clicking it, you will be able to see all the details of the vulnerability corresponding to a particular CVE ID.

How Network Configuration Manager categorizes firmware vulnerabilities

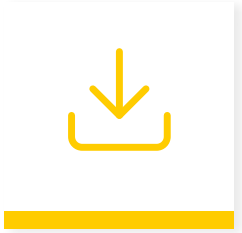


Summary

ManageEngine Network Configuration Manager provides effective firmware management with its top-notch, detailed listing of devices. With its advanced features, users can be informed about all the vulnerabilities in their network, find suitable patches, and apply them immediately instead of searching the NIST to find out about a vulnerability.

Network Configuration Manager also categorizes by severity and lets you know which vulnerability requires immediate attention.

If you are struggling to reduce firmware-vulnerability-related attacks, explore Network Configuration Manager now!



Download Free Trial

Request Demo

Get Price Quote