hack4glarus-2023-summer - Task #11853

Identify and illustrate potential operational and security risks associated with IPv6 in networks that are believed to be exclusively running IPv4 (OT/IoT-networks).

07/07/2023 06:15 PM - Mischa Diehm

Status:	Closed	**Start date:**	07/07/2023
Priority:	Normal	**Due date:**	07/09/2023
Assignee:	Mischa Diehm	**% Done:**	70%
Category:		**Estimated time:**	40.00 hours
Target version:			
PM Check date:			

Description

Focus on data-retrieval that can be passively collected (for example through CLI 'show' commands) from existing network infrastructure, which includes switches, routers, and firewalls. Initiate the investigation with air-gapped, non-routed networks.

For reference and as a starting point, use Eric Vyncke's paper titled 'The Layer-2 Security Issues and the Mitigation Techniques' (https://ripe65.ripe.net/presentations/129-vyncke_-_layer-2_security_ipv6_RIPE65.pptx.pdf)."

History

#1 - 07/09/2023 07:24 AM - Mischa Diehm

1. Considerations running networks with ipv6 enabled

When running networks with the belief that IPv6 is not configured, there are important operational and security considerations to keep in mind:

1. **Operational Considerations**:
- Network Visibility: Ensure proper monitoring and visibility tools are in place to detect IPv6 traffic, even if you believe it is not configured. This helps identify any unintended or unauthorized IPv6 activity.
- Configuration Audits: Regularly audit network devices and configurations to ensure there are no hidden or misconfigured IPv6 settings that may impact network operations or security.
- Documentation and Training: Maintain up-to-date documentation and provide training to network administrators and support staff about IPv6 and its potential impact on network operations.

2. **Security Considerations**:
- Addressing and Firewalling: Implement proper IPv6 address management and ensure that firewalls are configured to control both IPv4 and IPv6 traffic. This prevents unauthorized access and helps maintain a secure network perimeter.
- Security Monitoring: Extend security monitoring and incident response capabilities to cover IPv6 traffic as well. Monitor for any potential security threats or vulnerabilities specific to IPv6.
- Access Control: Review and update access control policies and mechanisms to account for the potential presence of IPv6 devices. Ensure that security controls are applied consistently across both IPv4 and IPv6 networks.
- Security Assessment: Conduct regular security assessments to identify any weaknesses or misconfigurations in both IPv4 and IPv6 environments. This helps proactively address security risks.

Remember, it's important to treat IPv6 as an integral part of your network infrastructure, even if you believe it is not actively configured. By considering these operational and security factors, you can better manage and secure your network environment.

1. ideas

1. **Consider Security Risks**: Completely discarding IPv6 or not monitoring it can introduce security problems. It's important to assess potential risks associated with the presence of IPv6 traffic, such as unauthorized access or security breaches.

2. **Detect Misconfigurations**: Regularly check for misconfigurations in the network that may inadvertently enable or expose IPv6. These misconfigurations can lead to unexpected network behavior or security vulnerabilities.

3. **Address Tunneling Traffic**: Be aware of potential tunneling techniques used to bypass network security measures. IPv6 tunneling can allow traffic to bypass security controls and reach the outside world. Implement appropriate security measures to monitor and control tunneling activities.

4. **Understanding Multicast Ping**: Investigate the concept of "Ping all devices in segment with all devices multicast." Understand how this mechanism works, as it may impact network performance and security. Consider its implications for network management and security policies.

5. **RA Guard and ND Guard**: Enable message logging for RA Guard to capture events related to unauthorized or invalid Router Advertisements (RAs). This logging feature can assist in troubleshooting and monitoring activities, providing valuable information for identifying and addressing potential security issues.

6. **Security risks keeping eyes closed**: think about security problems that are possible when totally discarding v6 or not monitoring this?

1. place a scan device in the network

If we have the opportunity to place an additional network scanner or sniffer within a segment, it can provide several advantages in terms of visibility, configuration validation, IPv6 usage assessment, and security. Here's a breakdown of the potential benefits:

1. **Visibility**: By deploying a scanner or sniffer, we gain enhanced visibility into the segment's network traffic. It allows us to monitor and analyze the communication patterns, identify devices, protocols, and services being used, and gain insights into the overall network behavior.

2. **Configuration Validation**: The scanner or sniffer can help validate the configuration of devices within the segment. We can assess if devices are properly configured, check for any misconfigurations, and ensure adherence to best practices. This assists in maintaining a consistent and secure network infrastructure.

3. **IPv6 Usage Assessment**: With the additional scanner or sniffer, we can specifically focus on analyzing IPv6 usage within the segment. It enables us to identify devices using IPv6, assess the effectiveness of IPv6 deployment, and identify any potential security vulnerabilities or misconfigurations related to IPv6.

4. **Security Analysis**: The scanner or sniffer enhances our ability to detect security threats and vulnerabilities within the segment. It allows us to monitor for suspicious network activities, identify potential security breaches, and investigate any unauthorized or malicious traffic. This helps in maintaining a robust security posture and responding promptly to security incidents.

In summary, by deploying an extra network scanner or sniffer within a segment, we gain improved visibility, configuration validation capabilities, insights into IPv6 usage, and enhanced security analysis. These benefits contribute to better network management, improved security practices, and a more efficient and secure network infrastructure.

1. Considerations / Problems / Questions

1. **Disabling IPv6 on Cisco IOS Router/Switch**:
- To disable IPv6 on Cisco IOS, you can use the "no ipv6 unicast-routing" command.

2. **IPv6 Traffic Not Filtered by Default**:
- By default, IPv6 traffic may not be filtered because its presence might not be recognized or assumed. It's essential to examine the router or firewall configuration to determine if IPv6 is allowed or blocked.

3. **SLAAC Default Behavior and MITM Vulnerability**:
- SLAAC (Stateless Address Autoconfiguration) has a default behavior that can make it easy to launch undetected or even unintentional Man-in-the-Middle (MITM) attacks. This highlights the importance of proper configuration and security measures for SLAAC-enabled networks.

4. **IPv6 Firewall Configuration**:
- Firewalls often have configurations specifically tailored for IPv4 but may lack similar restrictions for IPv6. It is crucial to ensure that IPv6 traffic is properly filtered and controlled, either through host-based or central firewall policies.

5. **Management Interfaces and Services Restrictions**:
- Management interfaces and services may have restrictions in place for IPv4, such as using Access Control Lists (ACLs), but similar restrictions may not be in effect for IPv6. It is important to review and update management policies to encompass IPv6 as well.

6. **Monitoring Systems and IPv6 Blind Spots**:
- Monitoring systems may primarily focus on IPv4 traffic and may not be fully aware of or capable of analyzing IPv6 traffic. This can create blind spots in monitoring and compromise the ability to detect and respond to potential threats in the IPv6 environment.

In summary, these points highlight important considerations related to IPv6 on Cisco IOS devices, including the need to disable IPv6, the default behavior and vulnerabilities of SLAAC, the configuration of firewalls and management interfaces/services for IPv6, and the potential blind spots in monitoring systems when it comes to IPv6 traffic. Addressing these concerns ensures proper network security, mitigates vulnerabilities, and maintains effective monitoring and management of both IPv4 and IPv6 traffic.

1. commands

1. cisco
   ```
   show ipv6 interface brief
   show ipv6 neighbors
   show ipv6 dhcp binding
   show ipv6 cef (features enabled)
   show ipv6 multicast (enabled?: ipv6 mfib)
   show ipv6 snooping intferface (show also if ra-guard is activated?)
   show mac address-table multicast address -> filter for 33:33:ff
   ```

#2 - 07/09/2023 07:25 AM - Mischa Diehm

- Status changed from New to Closed

#3 - 07/09/2023 08:41 AM - Mischa Diehm

- % Done changed from 0 to 70

#4 - 07/09/2023 10:16 AM - Mischa Diehm

- File md-hack4glarus.pdf added

Files

md-hack4glarus.pdf	682 KB	07/09/2023	Mischa Diehm