The core switch was attacked by this attack

Article Overview

The core switch was likely targeted by attacks such as MAC address flooding, ARP spoofing, VLAN hopping, or exploitation of specific switch vulnerabilities leading to denial of service or remote code execution.

Common Switch Attacks

MAC Address Flooding: Attackers overwhelm the switch's content addressable memory (CAM) table with fake MAC addresses, forcing the switch to broadcast all traffic to every port. This effectively turns the switch into a hub, allowing attackers to capture sensitive network traffic and monitor communications across the network . ARP Spoofing (ARP Poisoning): The attacker sends falsified ARP messages to associate their MAC address with the IP address of legitimate devices. This enables interception, modification, or disruption of data between devices, potentially allowing a man-in-the-middle attack . VLAN Hopping: By exploiting switch features, attackers can gain access to traffic on VLANs that are normally isolated. This can lead to unauthorized access to sensitive data and lateral movement within the network . Exploitation of Switch Vulnerabilities: Certain switches, such as Cisco Nexus 9000 Series in ACI mode or Cisco Catalyst 9300 series, have vulnerabilities that can be exploited by sending crafted Ethernet frames or abusing exposed SNMP services. These attacks can cause denial of service (DoS) or allow remote code execution, particularly if the management interface is exposed or unpatched .

Impact and Mitigation

Attacks on a core switch are critical because they can compromise the entire network's integrity. Potential impacts include network downtime, data interception, and unauthorized access to multiple VLANs. Mitigation strategies include:

o Using secure management protocols (SSH, HTTPS) instead of Telnet or HTTP .
o Implementing port security to limit valid MAC addresses per port .
o Segregating traffic with VLANs to contain potential breaches .
o Regularly updating switch firmware and applying security patches .
o Avoiding exposure of management interfaces to untrusted networks . Understanding these attack vectors helps network administrators strengthen defenses and reduce the risk of compromise to critical network infrastructure.

A group believed to be Russia"s Cozy Bear gained access to government and other systems through a compromised

The core switch was attacked by this attack

You can disable the forcefield in the CORE by either solving the puzzle (Sage"s Path) or battling monsters and flipping

Attackers use the compromised core switches to connect different VLANs by adding routing rules, then impersonate

A recent investigation by Kaspersky researchers into the APT group Awaken Likho (aka Core Werewolf and

301 Moved Permanently 301 Moved Permanently cloudflare

Operation Zero Disco hijacks Cisco switches via a critical SNMP flaw, installing an undetectable rootkit for total,

FEGtoken was attacked on #Ethereum, #BSC, and #Base last Sunday, resulting in losses exceeding $900K. As the

In this chapter, you will examine how Ethernet switches forward traffic, perform a controlled CAM table overflow attack, and

Dear All, I have Core Switch 4506 and i have 2 vlan : vlan 2 : 192.168.1.2 255.255.255.0 vlan 10 : 192.168.10.2

Hier sollte eine Beschreibung angezeigt werden, diese Seite lässt dies jedoch nicht zu.

Unsecured switches are vulnerable to susceptible attacks, causing downtimes. Thus, by implementing security

A vulnerability in the bootloader of Cisco IOS XE Software for Cisco Catalyst 9200 Series Switches, Cisco Catalyst ESS9300

CVE-2026-41089 Detail Description Stack-based buffer overflow in Windows Netlogon allows an unauthorized

The attack was the result of a Border Gateway Protocol (BGP) announcement that appeared to originate from the

The auditor is valid in raising this, because the switch being attacked is a core switch and so even if the attack surface is minimal, the

If your router is compromised, an attacker can pivot to your core switch without ever going through a firewall.

The core switch was attacked by this attack

What you"re saying is

Web: https://www.millstraining.co.za