From: **US-CERT** US-CERT@ncas.us-cert.gov
Subject: TA16-250A: The Increasing Threat to Network Infrastructure Devices and Recommended Mitigations
Date: September 7, 2016 at 12:22 AM
To: j2sw@mtin.net

National Cyber Awareness System:

TA16-250A: The Increasing Threat to Network Infrastructure Devices and Recommended Mitigations

09/06/2016 06:29 PM EDT

Original release date: September 06, 2016

Systems Affected

Network Infrastructure Devices

Overview

The advancing capabilities of organized hacker groups and cyber adversaries create an increasing global threat to information systems. The rising threat levels place more demands on security personnel and network administrators to protect information systems. Protecting the network infrastructure is critical to preserve the confidentiality, integrity, and availability of communication and services across an enterprise.

To address threats to network infrastructure devices, this Alert provides information on recent vectors of attack that advanced persistent threat (APT) actors are targeting, along with prevention and mitigation recommendations.

Description

Network infrastructure consists of interconnected devices designed to transport communications needed for data, applications, services, and multi-media. Routers and firewalls are the focus of this alert; however, many other devices exist in the network, such as switches, load-balancers, intrusion detection systems, etc. Perimeter devices, such as firewalls and intrusion detection systems, have been the traditional technologies used to secure the network, but as threats change, so must security strategies. Organizations can no longer rely on perimeter devices to protect the network from cyber intrusions; organizations must also be able to contain the impact/losses within the internal network and infrastructure.

For several years now, vulnerable network devices have been the attack-vector of choice and one of the most effective techniques for sophisticated hackers and advanced threat actors. In this environment, there has never been a greater need to improve network infrastructure security. Unlike hosts that receive significant administrative security attention and for which security tools such as anti-malware exist, network devices are often working in the background with little oversight—until network connectivity is broken or diminished. Malicious cyber actors take advantage of this fact and often target network devices. Once on the device, they can remain there undetected for long periods. After an incident, where administrators and security professionals perform forensic analysis and recover control, a malicious cyber actor with persistent access on network devices can reattack the recently cleaned hosts. For this reason, administrators need to ensure proper configuration and control of network devices.

Proliferation of Threats to Information Systems

SYNful Knock

In September 2015, an attack known as SYNful Knock was disclosed. SYNful Knock silently changes a router's operating system image, thus allowing attackers to gain a foothold on a victim's network. The malware can be customized and updated once embedded. When the modified malicious image is uploaded, it provides a backdoor into the victim's network. Using a crafted TCP SYN packet, a communication channel is established between the compromised device and the malicious command and control (C2) server. The impact of this infection to a network or device is severe and most likely indicates that there may be additional backdoors or compromised devices on the network. This foothold gives an attacker the ability to maneuver and infect other hosts and access sensitive data.

The initial infection vector does not leverage a zero-day vulnerability. Attackers either use the default credentials to log into the device or obtain weak credentials from other insecure devices or communications. The implant resides within a modified IOS image and, when loaded, maintains its persistence in the environment, even after a system reboot. Any further modules loaded by the attacker will only exist in the router's volatile memory and will not be available for use after the device reboots. However, these devices are rarely or never rebooted.

To prevent the size of the image from changing, the malware overwrites several legitimate IOS functions with its own executable code. The attacker examines the functionality of the router and determines functions that can be overwritten without causing issues on the router. Thus, the overwritten functions will vary upon deployment.

The attacker can utilize the secret backdoor password in three different authentication scenarios. In these scenarios the implant first checks to see if the user input is the backdoor password. If so, access is granted. Otherwise, the implanted code will forward the credentials for normal verification of potentially valid credentials. This generally raises the least amount of suspicion. Cisco has provided an alert on this attack vector. For more information, see the Cisco SYNful Knock Security Advisory.

Other attacks against network infrastructure devices have also been reported, including more complicated persistent malware that silently changes the firmware on the device that is used to load the operating system so that the malware can inject code into the running operating system. For more information, please see Cisco's description of the evolution of attacks on Cisco IOS devices.

Cisco Adaptive Security Appliance (ASA)

A Cisco ASA device is a network device that provides firewall and Virtual Private Network (VPN) functionality. These devices are often deployed at the edge of a network to protect a site's network infrastructure, and to give remote users access to protected local resources.

In June 2016, NCCIC received several reports of compromised Cisco ASA devices that were modified in an unauthorized way. The ASA devices directed users to a location where malicious actors tried to socially engineer the users into divulging their credentials.

It is suspected that malicious actors leveraged CVE-2014-3393 to inject malicious code into the affected devices. The malicious actor would then be able to modify the contents of the Random Access Memory Filing System (RAMFS) cache file system and inject the malicious code into the appliance's configuration. Refer to the Cisco Security Advisory Multiple Vulnerabilities in Cisco ASA Software for more information and for remediation details.

In August 2016, a group known as "Shadow Brokers" publicly released a large number of files, including exploitation tools for both old and newly exposed vulnerabilities. Cisco ASA devices were found to be vulnerable to the released exploit code. In response, Cisco released an update to address a newly disclosed Cisco ASA Simple Network Management Protocol (SNMP) remote code execution vulnerability (CVE-2016-6366). In addition, one exploit tool targeted a previously patched Cisco vulnerability (CVE-2016-6367). Although Cisco provided patches to fix this Cisco ASA command-line interface (CLI) remote code execution vulnerability in 2011, devices that remain unpatched are still vulnerable to the described attack. Attackers may target vulnerabilities for months or even years after patches become available.

Impact

If the network infrastructure is compromised, malicious hackers or adversaries can gain full control of the network infrastructure enabling further compromise of other types of devices and data and allowing traffic to be redirected, changed, or denied. Possibilities of manipulation include denial-of-service, data theft, or unauthorized changes to the data.

Intruders with infrastructure privilege and access can impede productivity and severely hinder re-establishing network connectivity. Even if other compromised devices are detected, tracking back to a compromised infrastructure device is often difficult.

Malicious actors with persistent access to network devices can reattack and move laterally after they have been ejected from previously exploited hosts.

Solution

1. Segregate Networks and Functions

Proper network segmentation is a very effective security mechanism to prevent an intruder from propagating exploits or laterally moving around an internal network. On a poorly segmented network, intruders are able to extend their impact to control critical devices or gain access to sensitive data and intellectual property. Security architects must consider the overall infrastructure layout, segmentation, and segregation. Segregation separates network segments based on role and functionality. A securely segregated network can contain malicious occurrences, reducing the impact from intruders, in the event that they have gained a foothold somewhere inside the network.

Physical Separation of Sensitive Information

Local Area Network (LAN) segments are separated by traditional network devices such as routers. Routers are placed between networks to create boundaries, increase the number of broadcast domains, and effectively filter users' broadcast traffic. These boundaries can be used to contain security breaches by restricting traffic to separate segments and can even shut down segments of the network during an intrusion, restricting adversary access.

Recommendations:

- Implement Principles of Least Privilege and need-to-know when designing network segments.
- Separate sensitive information and security requirements into network segments.
- Apply security recommendations and secure configurations to all network segments and network layers.

Virtual Separation of Sensitive Information

As technologies change, new strategies are developed to improve IT efficiencies and network security controls. Virtual separation is

the logical isolation of networks on the same physical network. The same physical segmentation design principles apply to virtual segmentation but no additional hardware is required. Existing technologies can be used to prevent an intruder from breaching other internal network segments.

Recommendations:

- Use Private Virtual LANs to isolate a user from the rest of the broadcast domains.
- Use Virtual Routing and Forwarding (VRF) technology to segment network traffic over multiple routing tables simultaneously on a single router.
- Use VPNs to securely extend a host/network by tunneling through public or private networks.

2. Limit Unnecessary Lateral Communications

Allowing unfiltered workstation-to-workstation communications (as well as other peer-to-peer communications) creates serious vulnerabilities, and can allow a network intruder to easily spread to multiple systems. An intruder can establish an effective “beach head” within the network, and then spread to create backdoors into the network to maintain persistence and make it difficult for defenders to contain and eradicate.

Recommendations:

- Restrict communications using host-based firewall rules to deny the flow of packets from other hosts in the network. The firewall rules can be created to filter on a host device, user, program, or IP address to limit access from services and systems.
- Implement a VLAN Access Control List (VACL), a filter that controls access to/from VLANs. VACL filters should be created to deny packets the ability to flow to other VLANs.
- Logically segregate the network using physical or virtual separation allowing network administrators to isolate critical devices onto network segments.

3. Harden Network Devices

A fundamental way to enhance network infrastructure security is to safeguard networking devices with secure configurations. Government agencies, organizations, and vendors supply a wide range of resources to administrators on how to harden network devices. These resources include benchmarks and best practices. These recommendations should be implemented in conjunction with laws, regulations, site security policies, standards, and industry best practices. These guides provide a baseline security configuration for the enterprise that protects the integrity of network infrastructure devices. This guidance supplements the network security best practices supplied by vendors.

Recommendations:

- Disable unencrypted remote admin protocols used to manage network infrastructure (e.g., Telnet, FTP).
- Disable unnecessary services (e.g. discovery protocols, source routing, HTTP, SNMP, BOOTP).
- Use SNMPv3 (or subsequent version) but do not use SNMP community strings.
- Secure access to the console, auxiliary, and VTY lines.
- Implement robust password policies and use the strongest password encryption available.
- Protect router/switch by controlling access lists for remote administration.
- Restrict physical access to routers/switches.
- Backup configurations and store offline. Use the latest version of the network device operating system and update with all patches.
- Periodically test security configurations against security requirements.
- Protect configuration files with encryption and/or access controls when sending them electronically and when they are stored and backed up.

4. Secure Access to Infrastructure Devices

Administrative privileges on infrastructure devices allow access to resources that are normally unavailable to most users and permit the execution of actions that would otherwise be restricted. When administrator privileges are improperly authorized, granted widely, and/or not closely audited, intruders can exploit them. These compromised privileges can enable adversaries to traverse a network, expanding access and potentially allowing full control of the infrastructure backbone. Unauthorized infrastructure access can be mitigated by properly implementing secure access policies and procedures.

Recommendations:

- Implement Multi-Factor Authentication – Authentication is a process to validate a user’s identity. Weak authentication processes are commonly exploited by attackers. Multi-factor authentication uses at least two identity components to authenticate a user’s identity. Identity components include something the user knows (e.g., password); an object the user has possession of (e.g., token); and a trait unique to the specific person (e.g., biometric).
- Manage Privileged Access – Use an authorization server to store access information for network device management. This type of server will enable network administrators to assign different privilege levels to users based on the principle of least privilege. When a user tries to execute an unauthorized command, it will be rejected. To increase the strength and robustness of user authentication, implement a hard token authentication server in addition to the AAA server, if possible. Multi-factor authentication increases the difficulty for intruders to steal and reuse credentials to gain access to network

multi-factor authentication increases the difficulty for intruders to steal and reuse credentials to gain access to network devices.

- Manage Administrative Credentials – Although multi-factor authentication is highly recommended and a best practice, systems that cannot meet this requirement can at least improve their security level by changing default passwords and enforcing complex password policies. Network accounts must contain complex passwords of at least 14 characters from multiple character domains including lowercase, uppercase, numbers, and special characters. Enforce password expiration and reuse policies. If passwords are stored for emergency access, keep these in a protected off-network location, such as a safe.

5. Perform Out-of-Band Management

Out-of-Band (OoB) management uses alternate communication paths to remotely manage network infrastructure devices. These dedicated paths can vary in configuration to include anything from virtual tunneling to physical separation. Using OoB access to manage the network infrastructure will strengthen security by limiting access and separating user traffic from network management traffic. OoB management provides security monitoring and can implement corrective actions without allowing the adversary who may have already compromised a portion of the network to observe these changes.

OoB management can be implemented physically or virtually, or through a hybrid of the two. Building additional physical network infrastructure is the most secure option for the network managers, although it can be very expensive to implement and maintain. Virtual implementation is less costly, but still requires significant configuration changes and administration. In some situations, such as access to remote locations, virtual encrypted tunnels may be the only viable option.

Recommendations:

- Segregate standard network traffic from management traffic.
- Enforce that management traffic on devices only comes from the OoB.
- Apply encryption to all management channels.
- Encrypt all remote access to infrastructure devices such as terminal or dial-in servers.
- Manage all administrative functions from a dedicated host (fully patched) over a secure channel, preferably on the OoB.
- Harden network management devices by testing patches, turning off unnecessary services on routers and switches, and enforcing strong password policies. Monitor the network and review logs Implement access controls that only permit required administrative or management services (SNMP, NTP SSH, FTP, TFTP).

6. Validate Integrity of Hardware and Software

Products purchased through unauthorized channels are often known as “counterfeit,” “secondary,” or “grey market” devices. There have been numerous reports in the press regarding grey market hardware and software being introduced into the marketplace. Grey market products have not been thoroughly tested to meet quality standards and can introduce risks to the network. Lack of awareness or validation of the legitimacy of hardware and software presents a serious risk to users’ information and the overall integrity of the network environment. Products purchased from the secondary market run the risk of having the supply chain breached, which can result in the introduction of counterfeit, stolen, or second-hand devices. This could affect network performance and compromise the confidentiality, integrity, or availability of network assets. Furthermore, breaches in the supply chain provide an opportunity for malicious software or hardware to be installed on the equipment. In addition, unauthorized or malicious software can be loaded onto a device after it is in operational use, so integrity checking of software should be done on a regular basis.

Recommendations:

- Maintain strict control of the supply chain; purchase only from authorized resellers.
- Require resellers to implement a supply chain integrity check to validate hardware and software authenticity.
- Inspect the device for signs of tampering.
- Validate serial numbers from multiple sources.
- Download software, updates, patches, and upgrades from validated sources.
- Perform hash verification and compare values against the vendor’s database to detect unauthorized modification to the firmware.
- Monitor and log devices, verifying network configurations of devices on a regular schedule.
- Train network owners, administrators, and procurement personnel to increase awareness of grey market devices.

Shadow Broker Exploits

Vendor	CVE	Exploit Name	Vulnerability
Fortinet	CVE-2016-6909	EGREGIOUSBLUNDER	Authentication cookie overflow
WatchGuard	CVE-2016-7089	ESCALATEPLOWMAN	Command line injection via ipconfig
Cisco	CVE-2016-6366	EXTRABACON	SNMP remote code execution
Cisco	CVE-2016-6367	EPICBANANA	Command line injection remote code execution
Cisco	N/A	BENIGNCERTAIN/PIXPOCKET	Information/memory leak
TOPSEC	N/A	ELIGIBLEBACHELOR	Attack vector unknown, but has an XML-like payload beginning with <?tos length="001e.%8.8x"?
TOPSEC	N/A	ELIGIBLEBOMBSHELL	HTTP cookie command injection
TOPSEC	N/A	ELIGIBLECANDIDATE	HTTP cookie command injection
TOPSEC	N/A	ELIGIBLECONTESTANT	HTTP POST parameter injection

References

- Cisco SYNful Knock Security Advisory
- Cisco Security Advisory Multiple Vulnerabilities in Cisco ASA Software
- Cisco Evolution of Attacks on Cisco IOS Devices
- Cisco IOS Software Integrity Assurance
- Information Assurance Advisory NO. IAA U/OO/802097-16 Mitigate Unauthorized Cisco ROMMON
- Information Assurance Advisory NO. IAA U/OO/802488-16 Vulnerabilities in Cisco Adaptive Security Appliances
- Information Assurance Directorate Network Mitigations Package – Infrastructure

Revision History

- September 6, 2016: Initial release
