Russian Cyber Attack Warning and Impact on AccessEnforcer® UTM Firewall

 | 800.650.8930 | info@calyptix.com

calyptix® SECURITY

U.S. and U.K. authorities last week alerted the public to an on-going effort to exploit network infrastructure devices – including routers, switches, and firewalls – by Russian state-sponsored actors.

The warning came as a technical alert (TA18-106A), the result of a joint effort by the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and the U.K. National Cyber Security Centre (NCSC).

Attackers have successfully exploited "large numbers" of enterprise-class and small home and office (SOHO) routers and switches, according to the alert. Information on the attacks has been gathered since 2015.

Systems affected:

- Cisco Smart Install (SMI) Enabled Devices
- Simple Network Management Protocol (SNMP) Enabled Network Devices
- Generic Routing Encapsulation (GRE) Enabled Devices

Targets are primarily:

- Government organizations
- Private sector organizations
- Critical infrastructure providers
- Internet service providers (ISPs)

The attackers typically establish a man-in-the-middle position once a device is compromised. This can grant broad power over the network, allowing them to extract or modify device configurations, create Generic Routing Encapsulation (GRE) tunnels, or redirect network traffic.

Attackers can also modify or deny a victim's network traffic in this scenario, however no reports of this have surfaced.

AccessEnforcer UTM Firewall Impact

Cisco Smart Install (SMI)

The most significant attacks described in the alert apply exclusively to Cisco devices running Cisco Internetwork Operating System (IOS). They do not affect AccessEnforcer.

This includes attacks leveraging Cisco Smart Install (SMI). SMI is an unauthenticated management protocol that allows administrators to download or overwrite files on any Cisco router or switch that supports the feature. AccessEnforcer does not support this protocol.

Simple Network Management Protocol (SNMP)

SNMP is an application-layer protocol used to monitor and manage devices on the network. SNMP versions 1 and 2 are not encrypted and pass information in plain text. Version 3 is encrypted. The technical alert describes attacks using SNMP versions 1 and 2 to gather reconnaissance data, steal passwords, and alter device configurations.

AccessEnforcer offers an SNMP agent (version 2) that is disabled by default. Once enabled, it makes available AccessEnforcer system data to SNMP monitoring tools. The agent listens for requests on IP addresses defined by the administrator and responds with system data.

The SNMP agent in AccessEnforcer is read-only. It cannot initiate management actions or configuration changes. The available system data is limited and does not include user information.

Device information that may be useful to an attacker's reconnaissance efforts can be gathered from an AccessEnforcer via SNMP – but only if **all of the following** conditions are met:

- An administrator has enabled the SNMP agent
- An attacker can reach the associated network and port on which the agent is listening
- The attacker knows the SNMP community string

This is why SNMP agents should never be enabled on a public WAN or other untrusted network. Also, SNMP community strings should follow best practices for password complexity (see additional information under "Recommendations").

Generic Routing Encapsulation (GRE)

GRE tunneling encapsulates one or more network protocols to create a point-to-point link between two end points. Attackers can use GRE tunnels to route traffic from a victim's system to a system they control.

AccessEnforcer does not support GRE tunnels. They cannot be established to or from the device. However, other devices on the network can create GRE tunnels to remote systems (assuming both endpoints support the protocol).

Additional Information

Below are excerpts from the technical alert describing other methods of cyber attack and comments on the impact to AccessEnforcer.

1. *"Login banners and other data collected from enabled services can reveal the make and model of the device and information about the organization for future engagement."*

   AccessEnforcer has two relevant services:

   - **GUI login –** the HTTPS login screen identifies the device as a Calyptix AccessEnforcer by default. No further specifics are provided.

     This page can be modified to remove any mention of AccessEnforcer, leaving only the text boxes for username and password. Remote management can also be limited to specific IP addresses, blocking access to this page by unauthorized hosts (see more under "Recommendations" below).

   - **SSH login –** this command-line login prompt reveals only that the device is an up-to-date OpenBSD/OpenSSH host with no further information.

2. *"Commercial and government security organizations have identified specially crafted SNMP and SMI packets that trigger the scanned device to send its configuration file…"*

   This vulnerability is specific to Cisco devices and does not affect AccessEnforcer.

3. *"In some cases, the actors use brute-force attacks to obtain Telnet and SSH login credentials"*

   Every AccessEnforcer is given a unique password of random characters at the time of manufacture. New passwords must contain at least seven characters and cannot contain only letters.

   All login attempts are entered in syslog with the corresponding source address.

4. *Protocols targeted in this scanning include:*

   - Telnet (TCP port 23 or a wide range others such as 80, 8080, etc.)
   - Hypertext Transport Protocol (HTTP port 80)
   - Simple Network Management Protocol (SNMP ports 161/162)
   - Cisco Smart Install (SMI port 4786).

These ports are closed on AccessEnforcer by default. If opened, connections can be limited to IP addresses or CIDRs specified by the administrator.

Recommendations for AccessEnforcer

AccessEnforcer has many features to prevent attacks of this type. The Calyptix development team will also incorporate further mitigations in coming releases of AccessEnforcer firmware to block similar threats.

We highly recommend the following configuration settings for AccessEnforcer to protect your network.

- Do not enable the SNMP agent unless necessary. If enabled, do not configure the agent to listen for requests on a public WAN or other untrusted network.
- Do not use simple or default phrases for any SNMP community string/name. Treat them as passwords and follow best practices for complexity.
- Restrict remote management to specific, trusted hosts.
- If using a default-allow policy for outbound filtering, create rules to block the following outbound ports:
    - » TCP & UDP 135 (MS RPC)
    - » TCP & UDP 137-139 (NetBIOS/IP)*
    - » TCP 445 (SMB/IP)*
    - » UDP 69 (TFTP)
    - » UDP 514 (Syslog)
    - » UDP 161-162 (SNMP)
    - » TCP 6660-6669 (Internet Relay Chat (IRC))
    - » TCP 4786 (SMI)
- Investigate or block inbound connections to the following WAN-side ports:
    - » TCP 23 (Telnet)
    - » UDP 69 (TFTP)
    - » UDP 161-162 (SNMP)
    - » TCP 4786 (SMI)

Also, be sure to patch or replace all aging network hardware, including modems, routers, switches, and firewalls.

*AccessEnforcer blocks outbound traffic on ports TCP 139 and TCP 445 by default. However, they can be opened with port forwarding and outbound filtering rules.