UK Internet Edge Router Devices: Advisory

You should read this advice if you are an internet service provider, or an enterprise that manages your own customer edge (CE) devices.

Summary

- This advice builds on existing technical guidance on the NCSC website.

- The NCSC is aware of a number of router compromises in telecommunications companies and Internet Service Providers, where a hostile actor has extracted configuration files from internet facing network devices. The configuration files can contain administrative credentials which may then be used to compromise all traffic passing through the router, and allow the actor to target other devices on the network. They have also gained interactive engineer access to some routers.

- In some cases where routers have been successfully compromised, the NCSC is aware that the hostile actor has created Generic Routing Encapsulation (GRE) tunnels to extract traffic traversing the router. They do this by using an Access Control List which they control on the compromised router, and exfiltrate the traffic they are interested in to infrastructure which they control, which is often outside the victim's country. In these cases where the NCSC is aware, we have already contacted the impacted organisations.

- The incident is still under investigation, and the NCSC is working with ISPs to make affected entities aware, and support remediation.

- This advisory note details mitigation strategies to secure networks against these attacks.

Details

The NCSC is aware of hostile actors accessing network devices using legitimate Simple Network Management Protocol (SNMP) credentials. Configuration files have subsequently been downloaded from the affected routers using the Trivial File Transfer Protocol (TFTP).

It has not yet been determined how these SNMP strings have been obtained.

Router configuration files can contain the router's administrative credentials, which may then be used to compromise all traffic on the router, and enable the actor to target other devices on the network. In some of the cases that NCSC is aware of, engineering credentials have been used by the hostile actors to access and change configuration on network devices.

There is currently no evidence to suggest that device firmware has been modified by the actors. Investigations on this aspect are ongoing.

Impact

In some cases where routers have been successfully compromised, the NCSC is aware that the hostile actor has created Generic Routing Encapsulation (GRE) tunnels to extract traffic traversing the router. In these cases where the NCSC is aware, we have already contacted the impacted organisations. They do this by using an Access Control List which they control on the compromised router, and exfiltrate the traffic they are interested in to infrastructure which they control, which is often outside the victim's country.

In practical terms, this means that the hostile actor will have access to, and visibility of, any traffic traversing that router. It does not necessarily mean that the actor will be able to read that traffic if it is encrypted.

Although we have no evidence to date, a compromised router can be used to modify traffic transiting it, or used as a beachhead to compromise the customer network itself.

The impact of a compromised router differs depending on where in an organisation's infrastructure it is located, and what functions it performs. Compromise of a router used as a site-to-site link is much more serious than one which is used as a gateway to the Internet. A site-to-site link router would have access to internal network traffic, which is likely to be less well protected, and might contain more sensitive data than traffic destined for the Internet. The devices which have been affected by this incident all have at least one direct internet accessible interface, but this does not rule out the possibility that some of them are being used for site-to-site connections. Affected ISPs are investigating the impact with their customers.

Mitigation

The NCSC has published comprehensive mitigation advice for Router compromises. However, more specific mitigation advice in relation to this recently observed activity is detailed as follows:

If you administer network devices which can be managed directly from the Internet:

Detecting a potential compromise

- Check logs for any evidence of tampering with the device – specifically instances of configurations being copied to a TFTP destination, redirection of command output to a TFTP destination, or the configuration of GRE tunnels linked to Access Control Lists. If any of these conditions are found, please contact the NCSC via the usual channels. Contact details for incident management can be found on the NCSC website (report a cyber security incident)

Preventing compromise

- Disable SNMP Read/Write if not strictly required (consider disabling SNMP entirely if not required).

- If SNMP Read/Write is required then at least one of the following two options must be put in place: EITHER ensure the SNMP service cannot be connected to untrusted sources OR upgrade to SNMPv3 and change all community strings.

- To ensure that the SNMP service cannot be connected to by an untrusted source, use an allow list Access Control List to restrict SNMP access to your network management platform only AND configure anti-spoofing at the edge of your network so that spoofed packets claiming to be sent from your network management platform are dropped.

- Ensure that interactive engineer access to network devices cannot occur from untrusted sources, by using allow list Access Control List (ACL) and anti-spoofing measures.

Remediation of a compromised device

- Consider following the device vendor's guidance on assuring the integrity of firmware, and then power-cycle the device.

If someone manages your Internet Facing Network Devices on your behalf, you should ask them the following questions. The comments below each question outline those conditions which MUST be in place as a mandatory requirement, as well as those which SHOULD be in place, but there may be valid reasons why they are not possible or required. You should also ask for information about the current, and historic, state of these features:

1. If SNMP is used on internet facing devices then how is it configured?

a) Unless required for specific functionality, SNMP must only be configured for Read-Only use.
b) Community Strings used with SNMP must be complex.
c) SNMP version 3 should be used
d) Community strings should be unique to each device, this may not be feasible depending on the management platform used.
e) If unique community strings are not feasible, ensure senior business risk owners are aware of how often community strings are shared, and how widely.

2. How do network engineers gain remote, interactive access to devices?

a) Remote engineer access must not use manufacturer default or company default credentials. (Passwords of Last Resort, when configured to require physical access, may use company shared credentials.)
b) Credentials for engineer remote access must be either unique to an engineer, or unique to a device.
c) Unique engineer credentials must not be stored on the network device.
d) Engineer interactive access must only be possible via strong, encrypted protocols (e.g. SSH v2 and HTTPS using TLS 1.2)
e) Multi-factor authentication should be required for remote engineer access (this can be on a specific management console which is the only point from which devices can be managed, rather than directly onto the device).
f) Engineers must administer devices from different endpoint devices from those that they use for general purposes (web browsing and email) and use credentials that are different from their general-purpose accounts.

3. How is logging configured on devices?

a) Show failed authentication attempts through any protocol, and be sufficient to identify brute-force attempts.
b) Logging must show valid authentication connections, including which network address the connection came from.
c) Logging must record any configuration changes made to a device by an engineer, down to specific commands used.
d) Logging must be centrally stored, off the network device in question.
e) Logging should be stored for a sufficient length of time to be useful for investigations.
f) You must specifically look for the indicators of compromise / attack that are listed previously in the advisory and ensure logs are actively monitored for suspicious activity

4. How is all administrative access (both interactive and programmatic) restricted?

- Administrative and engineering access via out of band or logically separated mechanisms are strongly preferred. If this is not possible, administrative and engineering access should be restricted via ACL functionality to specific network management systems.

5. Hardware device support and maintenance

- Security updates for these devices must be actively provided by the manufacturer.
- All devices must have relevant patches installed as quickly as possible.

Note: Some of the items listed in this section may incur additional costs or have impact on availability.

PUBLISHED

11 August 2017

REVIEWED

15 November 2018