CommScope / ARRIS is committed to the security of our devices and the millions of subscribers/customers who use them.

Tenable publicly disclosed a pair of vulnerabilities (from this point on in the document, we will refer to them as the Tenable vulnerabilities). These vulnerabilities can result in control over CPE devices including the following:

- Changing the configuration
- Loading malware

**Tenable/Password vulnerability:**

- A CPE device's graphical user interface (GUI) requires the user to enter the current password before proceeding to change/update the password. A post message can be sent directly to the device's web server to change the password, bypassing the client-side logic.
- This exploit requires a valid user session to be active and lowers the impact of this vulnerability; however, this vulnerability along with the lack of cross-site scripting request forgery (CSRF) protection makes this vulnerability high impact.

**Tenable/CSRF vulnerability:**

- With the lack of CSRF protections, this permits access to the device without authorization or authentication. A simple point-of-contact (PoC) web page can be built that can make configuration changes such as changing the administrator's password.
- This web page can be used to trick a user to click a link which would change the password without the user's consent or knowledge.

The vulnerabilities cannot be exploited from the public internet. The vulnerabilities can only be exploited from within a user's private network and requires device access from within that user's private network.

Specifically, the vulnerabilities impact the following products in Retail:

- ARRIS SURFboard SB8200 DOCSIS 3.1 cable modem

CommScope / ARRIS takes all vulnerabilities seriously. For the SB8200 unit, our team will have a firmware for the Tenable/Password vulnerability for service providers by mid-November. For the Tenable/CSRF vulnerability, our firmware was completed, and several service providers are currently deploying it and others will deploy it later.

DOCSIS standards dictate that the service provider must distribute firmware updates to cable modem devices. The end user cannot simply install an update like most other network-enabled devices.

In the meantime, end users/subscribers can minimize exposure by:

- Changing default passwords on home networking IoT devices (e.g., smart homes, smart security systems, surveillance cameras)
- Updating IoT and personal computing devices (e.g., PCs, mobile phones, tablets) to latest software versions
- Keeping anti-virus and anti-malware software updated on personal computing devices

###