Exodus Vulnerability

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

Exodus Intelligence publicly disclosed a vulnerability on Feb 10, 2022 ("Exodus vulnerability"). This vulnerability can result in the exploitation of the Simple Service Discovery Protocol (SSDP) by sending specialized extensible markup language (XML) to the SSDP on the device which leverages a command-injecting flaw.

This vulnerability must be exploited from the private network (LAN-side) and cannot be exploited from the public internet.

CommScope takes all vulnerabilities seriously. A firmware patch was developed, and we are evaluating other mitigation approaches to minimize the potential impact of the Exodus vulnerability.

What is the Exodus vulnerability?
This vulnerability must be exploited from the private network (LAN-side) and cannot be exploited from the public internet. This vulnerability can result in the exploitation of the Simple Service Discovery Protocol (SSDP) by sending specialized extensible markup language (XML) to the SSDP on the device and leveraging a command-injecting flaw.

How is CommScope responding to the Exodus vulnerability?
As soon as we learned of this latest vulnerability, we took the issue seriously and began assessing applicability to our products, and where necessary, developing firmware patches. We also evaluated other mitigation approaches to minimize the potential impact of Exodus vulnerability.

What CommScope products are vulnerable?

- **Home Networks Business Segment Products:**
  - ARRIS SURFboard Retail Products
    - SBG10 DOCSIS 3.0 cable modem and Wi-Fi router
    - SBG6950AC2 DOCSIS 3.0 cable modem and Wi-Fi router
    - SBG7400AC2 DOCSIS 3.0 cable modem and Wi-Fi router
    - SBG7580AC DOCIS 3.0 cable modem and Wi-Fi router
    - SBG7600AC2 DOCSIS 3.0 cable modem and Wi-Fi router

Is this issue limited to CommScope products?
The Exodus vulnerability applies to many products in the market. With respect to CommScope specific products, the Exodus vulnerability applies to the referenced CommScope products.

When will a solution/firmware update be available?
A firmware update was completed and made available 11.2021 to all service providers for deployment.

Why do you rely on service providers to apply your security updates when they could delay their release, putting end users'/subscribers' security at risk? Why can't CommScope release them directly to end users'/subscribers' devices?
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

case of detected device vulnerabilities, CommScope must develop the software update and make it available to service providers. The service providers qualify, test, and distribute the software update to devices on their network. CommScope has limited control or visibility on distribution by the service providers.

Who is Exodus Intelligence?
Based out of Austin, TX, Exodus Intelligence is cyber exposure company that provides customers with actionable information about the unknown vulnerabilities posing the greatest risk to their assets before malicious actors discover and exploit them.

Will CommScope devices in the field become worthless? Will they need to be discarded?
No. CommScope devices in the field will not become worthless. All CommScope devices have the capability to have their software images remotely upgraded by the service provider.

How can an end user/subscriber tell if he/she has received a security update and his/her device is now safe?
An end user/subscriber can check with their service providers and determine if an update is required for their device.

###