FOR IMMEDIATE RELEASE

SSDP Vulnerability

Comtrend Security Advisories, Responses, and Notices

Classification: SSDP Vulnerability

Advisory ID: Comtrend-SSDP-01.15

Public Release Date: October 7, 2014

Revision 1.0

Overview:

There has been a recent resurgence of illicit Internet activity that is affecting DSL gateways still using Broadcom's bcm63xx reference code. It is categorized as a SSDP Vulnerability that impedes the gateway's ability to communicate on the Internet. This bulletin offers solutions for the models using earlier versions of code and offers best-practice reminders to guard against this and related attacks in the future.

Issue Summary

Flaws in an older version of Broadcom bcm63xx reference code(s) were found to contain a vulnerability that can be compromised from SSDP inquires on the WAN side. This can result in a Distributed/Denial-of-Service (DoS and/or DDoS) attack that reduces available bandwidth. A router that utilizes firmware derived from bcm63xx reference code is most likely vulnerable to this type of attack.

Solutions:

1) Gateways should be upgraded to the latest release of software to close this vulnerability. Contact your Field Application Engineer to determine the availability of software for your model, and then upgrade the router to remove this vulnerability. Custom software may be built per normal procedure.

2) A few legacy products require software that will be categorized as beta. Custom software may be built upon these versions per normal procedure.

3) Service Providers (and end-users with appropriate router access) can turn on the firewall function. This setting prevents the DoS attack vulnerability, but may affect some applications.

Best Practice solutions include staying up to date with the latest software releases. We recommend that all Comtrend Customers subscribe to Comtrend's Technical Bulletins (here) to be advised of future software releases.

For Your Assistance:

Concerned service providers are encouraged to contact their Comtrend sales and field application engineer contacts to verify that their software is already patched against this vulnerability.

Email: na.support@comtrend.com

OR

Your Field Application Engineer:

- Gerard.Sison@Comtrend.com, National Accounts
- Joseph.Pessy@Comtrend.com, US & Canada
- Mario.Salgado@Comtrend.com, LATAM & Caribbean

We appreciate our technical support community and encourage direct communication with your sales and field application engineer contacts above. If you have any comments or questions about the technical bulletin, our newsletter and/or mailing lists, please email us at ComtrendConnection@comtrend.com

---

The contents of this document are current as of the date of publication. Comtrend Corporation reserves the right to change the contents without prior notice. In no event will Comtrend Corporation be liable for any damages or for commercial losses resulting from information contained in this document.

Comtrend Corporation
14 Chrysler
Irvine, CA 92618
(949) 753-9640

Additional Comtrend Resources

Early Adopter Program
Customer/Partners aiding in product development

Product Selector
Live product filtering by features and/or technology

Comtrend YouTube Channel
Support videos and training webinars

COMTREND
Leading the Communication Trend

www.Comtrend.com 14 Chrysler | Irvine CA 92618 | (877) COMTREND

Join Our Mailing List!