Extreme Networks ("Extreme") publishes vulnerability notes for our constituents to provide information and to raise awareness of particular issues deemed important to the security and integrity of the Extreme product set.

Release Date: 04/11/2014
Last Updated: 04/15/2014

Overview

US-CERT (United States Computer Emergency Readiness Team) has informed Extreme Networks of a potential OpenSSL vulnerability (VU#720951) where OpenSSL 1.0.1 contains a vulnerability that could disclose sensitive private information to an attacker. This vulnerability is commonly referred to as "heartbleed". Certain Extreme products as identified herein incorporate a version of the OpenSSL package affected by this vulnerability.

Products Affected

Products listed in the subsection below have been determined by Extreme to be affected by this vulnerability. Additional products will be added to the list below in the event determined to be affected.

- Black Diamond Series X8, 8900 and 8800 running EXOS version 15.4.1
- Summit Series X770, X670, X480, X460, X440, X430, E4G-200 and E4G-400 running EXOS version 15.4.1
- 64-bit (Ubuntu) hardware-based and virtual NetSight appliances; running versions 4.4, 5.0, 5.1, or 6.0
- 64-bit (Ubuntu) hardware-based and virtual NAC & IA appliances; running versions 5.0, 5.1, or 6.0
- 64-bit (Ubuntu) hardware-based and virtual Purview appliances; running version 6.0

Note: No other Extreme products (including the Enterasys-branded products) have been determined to be vulnerable at this time.

Description

A vulnerability in OpenSSL could allow a remote attacker to expose sensitive data, possibly including user authentication credentials and secret keys, through incorrect memory handling in the TLS heartbeat extension. This may allow an attacker to decrypt traffic or perform other attacks. OpenSSL version 1.0.1g resolves this vulnerability. The 1.0.0 and lower versions are not vulnerable.

Impact

The vulnerability impact on Extreme products and technologies identified herein varies depending upon the affected product and its use configuration and environment.

- ExtremeXOS version 15.4.1.x is affected. A patch update for ExtremeXOS 15.4.1.3-patch1-10 or higher is available for download.
- 64 bit (Ubuntu) NetSight Appliance version 4.4, 5.0, 5.1 6.0. A patch update is currently available for 4.4, 5.0, 5.1 & 6.0. Please contact the Extreme Networks Global Technical Assistance Center (GTAC) for access to the patch in the event not posted on the Extreme support site.
- 64 bit (Ubuntu) NAC Appliance version 5.0, 5.1, 6.0. A patch update is currently available for 5.0, 5.1 & 6.0. Please contact the Extreme Networks Global Technical Assistance Center (GTAC) for access to the patch in the event not posted on the Extreme support site.

- 64 bit (Ubuntu) Purview Appliance version 6.0. A patch update is currently available. Please contact the Extreme Networks Global Technical Assistance Center (GTAC) for access to the patch in the event not posted on the Extreme support site.

Note: Except as identified herein, no other Extreme products (including the Enterasys-branded products) have been determined to be vulnerable at this time.

Repair Recommendation

Ensure that the Extreme switches/routers and the NetSight Management Suites are running the latest firmware & software releases. Workarounds to mitigate the heartbleed vulnerability may be available.

Firmware & Software can be downloaded from - https://www.extremenetworks.com/support/

Legal Notice

THIS ADVISORY NOTICE IS PROVIDED ON AN "AS IS" BASIS AND EXTREME MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, EXPRESSLY DISCLAIMING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. USE OF THE INFORMATION PROVIDED HEREIN OR MATERIALS LINKED FROM THIS ADVISORY NOTICE IS AT YOUR OWN RISK. EXTREME RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME, AND EXPECTS TO UPDATE THIS DOCUMENT AS NEW INFORMATION BECOMES AVAILABLE. THE INFORMATION PROVIDED HEREIN IS APPLICABLE TO CURRENT EXTREME PRODUCTS SUBJECT HEREIN AND IS NOT INTENDED TO BE ANY REPRESENTATION OF FUTURE FUNCTIONALITY OR COMPATIBILITY WITH ANY 3RD PARTY TECHNOLOGIES REFERENCED HEREIN.