6605 19 ½ Mile Road
Sterling Heights, MI 48314-1408 USA
Tel: +1-586-254-0020 | Fax: +1-586-254-0053
info@sisconet.com | www.sisconet.com

Security Update Notification

Vulnerability Disclosure for CVE-2015-6574
26 April 2016

Background

While testing for a client, Portcullis Computer Security, Ltd. detected a vulnerability in SISCO's MMS-EASE V11.2000 product for RedHat Linux. SISCO was notified of the vulnerability on 29 July 2015 and determined that both MMS-EASE and AX-S4 ICCP products that contained the numeral "142" in the part number were impacted/affected. In January of 2016, Portcullis posted a public disclosure of this vulnerability to its website. SISCO customers were notified of the vulnerability and provided with a patch prior to that public disclosure. This notice is in response to that public disclosure.

Details of all corrections made to SISCO products are documented in the release notes that accompany the product.

Description

The vulnerability is a 'remote denial of service' where a specially-crafted packet would cause the SNAP Lite component of the SISCO product (with or without the security extensions) to consume all CPU cycles that were available to it, thereby making the communications stack unresponsive to further communications.

Mitigation and Risk

The only known mitigation is to update the affected software to the latest available version (see below). The risk associated with this vulnerability can be reduced by ensuring that only trusted computers have access to the network by using VPN technology to control access to the ICCP network. For systems where unauthorized access to the ICCP network is prevented through the use of up-to-date VPN technology, the risk of this vulnerability impacting system operation is low.

Notes on Products, Part Numbers and Versions

The MMS-EASE products affected are designated with a part number "MMS-SECURE-142-XXX-DEV" where the 'XXX' indicates the computing platform on which the product is designed to run as described in the table below. SISCO refers to this product generically as the "MMS-EASE" development license. MMS-EASE is used to develop ICCP-TASE.2 products by a variety of EMS/SCADA suppliers. These EMS/SCADA suppliers embed executable versions of the MMS-EASE product in their own ICCP-TASE.2 products which are then distributed to end users. The executable versions of the products distributed to end users are designated with part numbers matching the development license and ending in suffixes such as –EXE, –EXEHB or –EXEADD. The prefix to the part numbers indicate if the executable license contains the security extensions ("MMS-SECURE") or if they do not ("MMS-EASE").

Also affected is V6.0000 of the AX-S4 ICCP product that includes "142-095" in the part number.

The vulnerability is in a component of the MMS-EASE and AX-S4 ICCP products called "SNAP Lite". This component is not sold separately and its version number is not generally referred to in technical support transactions with SISCO. Version numbers are based on the full product and SISCO does not publish individual component version numbers. This may cause some confusion as the Portcullis advisory refers to a version number of the SNAP Lite component only.

Patch Versions

The following table identifies the part and version numbers of the products that have been patched to include a mitigation for this vulnerability. Any product identified by the part number in the following table that is an earlier version than indicated will need to be updated to address this vulnerability. SISCO products that do not match the part numbers shown below are not affected.

Product Name and Description	Part Numbers of Affected Products			Available Patch	
	Prefix	Platform Number	Suffix	Version	Date Released
MMS-EASE for RedHat Linux	MMS-SECURE or MMS-EASE	142-764 or 142-700	-DEV -EXE -EXEHB -EXEADD	V11.2000.2	3 Sept 2015
MMS-EASE for Windows	MMS-SECURE or MMS-EASE	142-064 or 142-095	-DEV -EXE -EXEHB -EXEADD	V11.8000.2	21 Sept 2015
MMS-EASE for AIX	MMS-SECURE or MMS-EASE	142-664 or 142-600	-DEV -EXE -EXEHB -EXEADD	V11.3000.3	14 Oct 2015
MMS-EASE for Solaris x86	MMS-SECURE or MMS-EASE	142-714 or 142-715	-DEV -EXE -EXEHB -EXEADD	V11.8000.1	2 Oct 2015
MMS-EASE for Solaris SPARC	MMS-SECURE or MMS-EASE	142-764 or 142-700	-DEV -EXE -EXEHB -EXEADD	V11.8000.1	2 Oct 2015
AX-S4 ICCP	AXS4-ICCP or AXS4-ICCP-SECURE	142-095	-DEV -PAK	V6.0200	1 Oct 2015

More Information

Portcullis Advisory URL: https://www.portcullis-security.com/security-research-and-downloads/security-advisories/cve-2015-6574/

For access to updates and patches for products that are purchased from other vendors that includes embedded versions of SISCO software (part number suffixes of -EXE, -EXEHB or -EXEADD) affected users should contact that vendor directly. Software patches from SISCO that are provided for a -DEV license cannot be directly applied to a system running a product containing an -EXE, -EXEHB or -EXEADD product.

SISCO customers with -DEV or -PAK licenses to the products listed above with active support and maintenance should log in to the SISCO support portal (https://portal.sisconet.com) to download available patches and access other technical support services as needed.

SISCO customers with -DEV or -PAK licenses to the products listed above without active support and maintenance products should contact the SISCO VAR from which they purchased their license (http://www.sisconet.com/partners) or SISCO directly at support@sisconet.com.

SISCO's security policy can be found on our web site at: http://www.sisconet.com/support/security