Xerox Multifunction Devices

Customer Tips

... for the user

Dc02cc0274
January 28, 2004

Xerox Response to CERT® Coordination Center SNMP Advisory

Purpose

This document describes an advisory issued by CERT® Coordination Center (CERT/CC) concerning Simple Network Management Protocol (SNMP) implementations. It also contains Xerox's response to the advisory.

Background

The CERT/CC has published an advisory located at: http://www.cert.org/advisories/CA-2002-03.html

The advisory states that numerous vulnerabilities have been reported in multiple vendors' Simple Network Management Protocol (SNMP) implementations. These vulnerabilities may cause unauthorized privileged access, denial-of-service conditions, service interruptions, unstable behavior and in some cases may allow an attacker to gain access to the affected device. Specific impacts vary from product to product.

CERT/CC is a center of Internet security expertise, at the Software Engineering Institute (http://www.sei.cmu.edu), a federally funded research and development center operated by Carnegie Mellon University (http://www.cmu.edu). They study Internet security vulnerabilities, handle computer security incidents, publish security alerts, research long-term changes in networked systems, and develop information and training to help you improve security at your site.

SNMP is a widely deployed protocol commonly used to monitor and manage network devices. Version 1 of the protocol (SNMPv1) defines several types of SNMP messages used to request information or configuration changes, respond to requests, enumerate SNMP objects, and send unsolicited alerts. The Oulu University Secure Programming Group (OUSPG) has reported numerous vulnerabilities in SNMPv1 implementations from many different vendors.

You can find more information about SNMP and OUSPG, focused on the manner in which SNMPv1 agents and managers handle request and trap messages, in OUSPG's research. OUSPG applied the PROTOS c06-snmpv1 test suite located at http://www.ee.oulu.fi/research/ouspg/protos/testing/c06/snmpv1/0100.html to a variety of popular SNMPv1-enabled products to reveal the following vulnerabilities.

This document pertains to these Xerox products:

x	WC Pro 32/40 Color
x	WC Pro 65/75/90
x	WC Pro 35/45/55
x	WC M35/M45/M55
x	DC 490/480/470/460 ST
x	DC 440/432/425/420 ST
x	DC 340/332 ST
x	DC 265/255/240 ST/LP
x	DC 230/220 ST/LP
x	DCCS 50

Multiple Vulnerabilities in SNMPv1 Trap Handling

SNMP trap messages are sent from agents to managers. A trap message may indicate a warning or error condition, or otherwise notify the manager about the agent's state. SNMP managers must properly decode trap messages and process the resulting data. In testing, OUSPG found multiple vulnerabilities in the way many SNMP managers decode and process SNMP trap messages.

Multiple Vulnerabilities in SNMPv1 Request Handling

SNMP request messages are sent from managers to agents. Request messages might be issued to obtain information from an agent or to instruct the agent to configure the host device. SNMP agents must properly decode request messages and process the resulting data. In testing, OUSPG found multiple vulnerabilities in the way many SNMP agents decode and process SNMP request messages.

Vulnerabilities in the decoding and subsequent processing of SNMP messages by both managers and agents may result in denial-of-service conditions, format string vulnerabilities, and buffer overflows. Some vulnerabilities do not require the SNMP message to use the correct SNMP community string.

Results of Tests on Xerox Document Centres

In response to the CERT advisory, Xerox ran the Protos Test Suite on our DCCS 50, DC 230/220, DC 340/332, DC240/255/265, DC 440/432/425/420, and the DC 490/480/470/460 products. No exploitable vulnerabilities were found and no SNMP related system failures or compromises to the Document Centre occurred as a result of performing these tests.

Additional Information

Xerox Customer Service welcomes feedback on all documentation - send feedback via e-mail to: USA.DSSC.Doc.Feedback@mc.usa.xerox.com.

You can reach Xerox Customer Support at 1-800-821-2797 (USA), TTY 1-800-855-2880 or at http://www.xerox.com.

Other Tips about Xerox multifunction devices are available at the following URL: http://www.xerox.com/DocumentCentreFamily/Tips.

THE DOCUMENT COMPANY
XEROX®