

## **Xerox Product Response for CERT Advisory CA-2002-03 *Multiple Vulnerabilities in Many Implementations of SNMP***

### **Audience and Purpose**

The primary audience for this document is Xerox analysts and customers who want information regarding how Xerox products respond to [CERT Advisory CA-2002-03](#) and Vulnerability Notes [VU#854306](#) and [VU#107186](#), issued by CERT on February 12, 2002. Xerox is working with CERT to the fullest extent possible, and has analyzed its fleet of products. The following sections provide as background excerpts from the CERT advisory, mitigating factors when considering this advisory and Xerox products, and responses from Xerox grouped according to product family.

### **Background**

The CERT<sup>®</sup> Coordination Center (CERT/CC) published an advisory that can be found at <http://www.cert.org/advisories/CA-2002-03.html>. The advisory states that numerous vulnerabilities have been reported in multiple vendors' 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 will vary from product to product.

The CERT<sup>®</sup> Coordination Center (CERT/CC) is a center of Internet security expertise, at the [Software Engineering Institute](#), a federally funded research and development center operated by [Carnegie Mellon University](#). 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.

The Simple Network Management Protocol (SNMP) is a widely deployed protocol that is commonly used to monitor and manage network devices. Version 1 of the protocol (SNMPv1) defines several types of SNMP messages that are 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.

OUSPG's research focused on the manner in which SNMPv1 agents and managers handle request and trap messages. By applying the PROTOS c06-snmpv1 test suite found at <http://www.ee.oulu.fi/research/ouspg/protos/testing/c06/snmpv1/0100.html> to a variety of popular SNMPv1-enabled products, the OUSPG revealed the following vulnerabilities:

- **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.

### **Mitigating Factors**

Xerox products range from software applications to desktop printers to multifunction devices and production printers. The vulnerability to this advisory will tend to vary. It is important to always read the additional information that is provided for the product family. Customers should understand the vulnerability of the operating system on their PC or workstation. In order to ensure the underlying operating system is not vulnerable, customers should check the appropriate vendor web site to assess the risk with respect to their work environment. If precautions suggested elsewhere in this CERT advisory are taken to secure networks and operating systems within a firewall, risk to operation of Xerox products may be minimal.

**Xerox Product Responses**

The following table lists Xerox responses to CERT Advisory by product family.

<b>Xerox Solutions and Software Products</b>		
<b>CentreWare Web, CentreWare MC and CentreWare DP, PrinterMap, PnP 2000</b>	Not Vulnerable	<p>These applications are not vulnerable. The customer can disable the SNMP service on the hosted server without affecting the operation of the application.</p> <p>Notes:</p> <ul style="list-style-type: none"> <li>• If SNMP traffic is disabled on the internal routers, these applications will be unable to obtain remote management information across the internal routers.</li> <li>• If SNMP is disabled on a printer, these applications will be unable to discover or manage that device.</li> </ul>
<b>EMS Solutions (IBM Tivoli NetView, HP Openview NNM, CA Unicenter)</b>	Not Vulnerable	<p>Xerox tested EMS Solutions as patches became available from our integration partners (IBM, Computer Associates, and Hewlett Packard). No vulnerabilities were found in CentreWare for IBM Tivoli NetView, CentreWare for CA Unicenter TNG, and CentreWare for HP OpenView NNM after patches were applied.</p> <p>Customers should refer to Computer Associates, Hewlett Packard and IBM for further information regarding Unicenter TNG, OpenView NNM and Tivoli NetView.</p>
<b>DigiPath, DocuShare, Flowport, mDoc</b>	Not Vulnerable	These applications do not use the SNMP protocol.
<b>DP Server for AIX</b>	Not Vulnerable	DP Server for AIX does not use the SNMP protocol.
<b>DP Server for NT and PrintXchange for NT</b>	See note	Xerox has tested DP Server and PrintXchange for NT, and vulnerabilities were found. A patch is required from Microsoft to restore the application to working order and prevent vulnerability.
<b>PrintXchange for Solaris and Windows 2000</b>	Not Vulnerable	Xerox has tested PrintXchange for Solaris and PrintXchange for Windows 2000, and no vulnerabilities were found
<b>CentreWare Network Services and CentreWare Scan Services</b>	Not Vulnerable	Xerox has run the PROTOS c06-SNMPv1 test suite on the CentreWare Network Services applications and CentreWare Scan Services applications, and no vulnerabilities were found.
<b>Xerox Printers and Multifunction Devices</b>		
<b>Document Centre products</b>	Not Vulnerable	Xerox has run the PROTOS c06-SNMPv1 test suite on Document Centre DCCS 50, DC 220/230, DC 332/340, DC240/255/265, DC 420/425, DC432/440, DC460/470, and the DC 480/490 series products, and no vulnerabilities were found.
<b>WorkCentre Pro products</b>	Not Vulnerable	Xerox has run the PROTOS c06-SNMPv1 test suite on the WorkCentre Pro 423/428 and WorkCentre Pro 580 products, and no vulnerabilities were found. The WorkCentre Pro 412 and WorkCentre Pro 580 products are not vulnerable; however, customers should verify that any external network connection hardware is not vulnerable.

<b>DocuSP-based products</b>	See note	<p>DocuSP 3.x The implementation of SNMP in DocuSP 3.x and higher software levels has been tested and is not vulnerable. If customers are running the Sun Solaris SNMP agent instead of the DocuSP SNMP agent, patch 106869-15 for Solaris 8 from Sun (Solstice Enterprise Master Agent) is available at <a href="http://www.sunsolve.sun.com">http://www.sunsolve.sun.com</a>. This patch from Sun is also planned for inclusion in a DocuSP 3.1 release.</p> <p>DocuSP 2.x In DocuSP 2.x the software is considered to be vulnerable. As recommended previously, DocuSP 2.x customers should consider removing SNMP from the controller. The SNMP agent from Sun should also be disabled. It is highly recommended that customers upgrade to a DocuSP 3.x release as soon as practical if SNMP is required.</p> <p>For DocuTech 61xx and DocuPrint EPS 2000 products, the DocuSP 3.1 software is currently available. For DocuTech/DocuPrint 65/75/90 products that are currently installed with DocuSP2.1 software, it is recommended that SNMP not be used.</p>
<b>DocuColor EX2000 Family (X12/XP12/EX12 EX2000/EX2000v /EX2000d)</b>	See note	No vulnerabilities were found in the DocuColor EX2000 Family after patches were applied from EFI. To obtain the patches, contact Xerox support.
<b>DocuColor 2045/2060(xx) with CSX2000</b>	Not Vulnerable	SNMP is not required and, therefore, Xerox recommends that customers disable SNMP on the CreoScitex CSX2000 Color Server.
<b>DocuPrint NPS Series</b>	See note	Xerox recommends that customers disable SNMP on their DocuPrint NPS Series printers. DocuPrint NPS release 7.3 will address this vulnerability for customers who require SNMP.
<b>Phaser and DocuPrint N Series Products</b>	See note	<p>The Xerox Office Printing Business team has evaluated several printers using the PROTOS test suite (c06-SNMPv1) provided by Oulu University. We have chosen a sampling of products which, due to the degree of code reuse, we believe to be a fair and accurate representation of all products in that family.</p> <p>The PROTOS test suite reported no errors or exceptions for this family of printers: DocuPrint N2025, DocuPrint N2125, DocuPrint N2825, DocuPrint N3225, DocuPrint N4025, DocuPrint N4525, Phaser 5400.</p> <p>The PROTOS test suite reported errors for this family of printers: Phaser 7700, Phaser 860, Phaser 850, Phaser 840, Phaser 780, Phaser 750, Phaser 740/740L, Phaser 360.</p> <p>The errors resulted in 2 printer states. Errors were detected within the printer and the printer automatically reset itself, or errors were detected and the SNMP stack was automatically disabled. When the printer was reset, it returned to a fully operational state with no loss or corruption of internal data. When the SNMP stack was disabled, the printer would no longer respond to SNMP packets, but remained fully functional in all other aspects. Printing was not affected.</p>

**Contact**

For additional information or clarification on any of the product information given here, contact Xerox support.

**Disclaimer**

The information provided in this Xerox Product Response is provided "as is" without warranty of any kind. Xerox Corporation disclaims all warranties, either express or implied, including the warranties of merchantability and fitness for a particular purpose. In no event shall Xerox Corporation be liable for any damages whatsoever resulting from user's use or disregard of the information provided in this Xerox Product Response including direct, indirect, incidental, consequential, loss of business profits or special damages, even if Xerox Corporation has been advised of the possibility of such damages. Some states do not allow the exclusion or limitation of liability for consequential damages so the foregoing limitation may not apply.