



December 18, 2007

McAfee, Inc.
McAfee® Avert® Labs Security Advisory
Public Release Date: 2007-12-18

CUPS Backend SNMP Remote Stack Buffer Overflow Vulnerability

CVE-2007-5849

- **Synopsis**

The CUPS backend SNMP program broadcasts SNMP requests to discover network print servers. A stack buffer overflow may result from an integer underflow in the handling of SNMP responses. If SNMP is enabled, a remote attacker may exploit this issue by sending a maliciously crafted SNMP response, which may cause an application termination or arbitrary code execution.

- **Vulnerable System or Application**

CUPS version 1.3.4 and Prior
CUPS version 1.2.12 and Prior

- **Vulnerability Information**

CVE-2007-5849

The vulnerability is caused due to a 'signedness' error within the "asn1_get_string()" function in backend/snmp.c. This can get triggered when the backend SNMP program is processing SNMP responses which are ASN.1 encoded strings. Successful exploitation allows execution of arbitrary code. A failed exploit attempt will cause the SNMP program to crash resulting in a Denial Of Service.

- **Resolution**

Update to version 1.3.5

- **Credits**

This vulnerability was discovered by Wei Wang of McAfee Avert Labs.

- **Legal Notice**

Copyright (C) 2007 McAfee, Inc.

The information contained within this advisory is provided for the convenience of McAfee's customers, and may be redistributed provided that no fee is charged for distribution and that the advisory is not modified in any way. McAfee makes no representations or warranties regarding the accuracy of the information referenced in this document, or the suitability of that information for your purposes.

McAfee, Inc. and McAfee Avert Labs are registered Trademarks of McAfee, Inc. and/or its affiliated companies in the United States and/or other Countries. All other registered and unregistered trademarks in this document are the sole property of their respective owners.