



December 19, 2007

McAfee, Inc.
McAfee® Avert® Labs Security Advisory
Public Release Date: 2007-12-19
Multiple integer overflows in e2fsprogs (Xen related)

CVE-2007-5497

- **Synopsis**

Multiple integer overflows in e2fsprogs allow for arbitrary code execution.

- **Vulnerable System or Application**

E2fsprogs <=1.40.2
Any application linked with vulnerable versions of libext2fs

- **Vulnerability Information**

CVE-2007-5497

When processing ext2 or ext3 filesystem, the vulnerable applications do not sanitize certain fields taken directly from the input filesystem. As the result, buffer sizes can be calculated incorrectly, which may lead to a heap overflow and execution of arbitrary code.

There are two possible exploitation vectors:

- 1) Enticing a user to process a maliciously crafted ext2 or ext3 filesystem with a vulnerable application
 - 2) Pygrub, an utility commonly used with Xen, parses the guest filesystem in order to extract the kernel and configuration files. The user with administrative privileges in the guest can create a malformed /boot partition, which may result in arbitrary code execution on the host when pygrub parses this partition after guest domain restart.
-

- **Resolution**

E2fsprogs-1.40.3 fixes this vulnerability.

- **Credits**

This vulnerability was discovered by Rafal Wojtczuk 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.