

Flaw Fixed in Unix-like Systems

A file integer underflow vulnerability could be exploited to trigger buffer overflow in unpatched Unix-like systems.

A buffer overflow vulnerability caused by an integer underflow in the file_printf function in Unix-like operating systems has been patched.

The flaw is contained within the file program and could allow an attacker to execute arbitrary code or create a denial of service condition, according to a posting on the United States Computer Emergency Readiness Team's Web site.

File is a program used to determine what type of data is contained in a file. To trigger the overflow, a hacker would need to get a user to run a vulnerable version of file on a specially crafted file, the advisory states.

"Version 4.20 of file was released to address this issue," according to the US-CERT advisory.

If exploited, an attacker could execute malicious code with the permissions of the user running the vulnerable version of file or cause the program to crash, creating a denial-of-service condition.

Patches by [Red Hat](#) and [Ubuntu](#) were released more than a week ago for users of Red Hat Enterprise Linux 4 and 5 as well as Ubuntu 5.10, Ubuntu 6.06 LTS, Ubuntu 6.10 and corresponding versions of Kubuntu, Edubuntu, and Xubuntu. OpenWall GNU/*Linux and Mandriva have also released updates to address the issue.

In addition, running the file program with a limited user account may partially address the impact of a successful exploit of the flaw.

Copyright 2007 by Ziff Davis Media, Distributed by United Press International

This document is subject to copyright. Apart from any fair dealing for the purpose of private study, research, no part may be reproduced without the written permission. The content is provided for information purposes only.