

# [VulnWatch] gfxboot allows boot password circumvention, SuSE 8.1 GRUB

*Source:* <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2002-12/0012.html>

---

*From:* Matthias Andree ([matthias.andree@gmx.de](mailto:matthias.andree@gmx.de))

*Date:* 12/14/02

Date: Sat, 14 Dec 2002 02:18:44 +0100

From: Matthias Andree <[matthias.andree@gmx.de](mailto:matthias.andree@gmx.de)>

To: [vulnwatch@vulnwatch.org](mailto:vulnwatch@vulnwatch.org), [bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com)

## SECURITY VULNERABILITY

SuSE 8.1's "gfxmenu" which is configured into GRUB by default on many machines allows the user to pass in additional kernel boot parameters without entering the password, even though one is configured in the GRUB configuration file. The exact circumstances when YaST2 adds the gfxmenu configuration have not been researched. What other machines may be affected, has not been researched either. SuSE used LILO up to and including SuSE Linux 8.0.

## HOW TO CHECK IF YOU ARE VULNERABLE

As no fix is known at the moment, just reading the /boot/grub/menu.lst configuration file is sufficient. If yours has a line that starts with "gfxmenu", the computer is vulnerable.

## IMPACT

A malicious user who can make the computer reboot can for example append `init=/bin/bash` to defeat the regular boot procedures to bypass the root password and steal data or install backdoors.

## FIX

Unknown.

## WORKAROUND

Remove the gfxboot line from /boot/grub/menu.lst.

## HISTORY AND FUTURE

2002-11-27 v1.0 initial announcement, disclosed to SuSE Security only.

2002-11-29 extended schedule to 2002-12-13, 24:00 GMT

2002-12-03 original schedule date for publication

VulnWatch: [VulnWatch] gfxboot allows boot password circumvention, SuSE 8.1 GRUB

2002-12-13 deadline. public announcement will be made on this day at the latest.

2002-12-13 v1.1 reword first paragraph, not all machines enable gfxmenu  
by default, add section on checking for the problem.

2002-12-14 sent this announcement to vulnwatch and bugtraq, a workaround  
is documented, so holding back the announcement makes no sense.