

# Revised OpenSSH Security Advisory (adv.token)

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2002-04/0387.html>

---

**From:** Markus Friedl ([markus@openbsd.org](mailto:markus@openbsd.org))

**Date:** 04/26/02

Date: Fri, 26 Apr 2002 13:59:49 +0200  
From: Markus Friedl <[markus@openbsd.org](mailto:markus@openbsd.org)>  
To: [BUGTRAO@SECURITYFOCUS.COM](mailto:BUGTRAO@SECURITYFOCUS.COM)

This is the 2nd revision of the Advisory.

Buffer overflow in OpenSSH's sshd if AFS has been configured on the system or if KerberosTgtPassing or AFSTokenPassing has been enabled in the sshd\_config file. Ticket and token passing is not enabled by default.

## 1. Systems affected:

All Versions of OpenSSH with AFS/Kerberos token passing compiled in and enabled (either in the system or in sshd\_config) contain a buffer overflow.

Token passing is disabled by default and only available in protocol version 1.

## 2. Impact:

Remote users can get privileged access for OpenSSH < 2.9.9

Local users can get privileged access for OpenSSH < 3.2.1

No privileged access is possible for OpenSSH with UsePrivilegeSeparation enabled.

## 3. Solution:

Apply the matching patch:

<ftp://ftp.openbsd.org/pub/OpenBSD/OpenSSH/openssh-3.1-adv.token.patch>  
<ftp://ftp.openbsd.org/pub/OpenBSD/OpenSSH/portable/openssh-3.1p1-adv.token.patch>  
[ftp://ftp.openbsd.org/pub/OpenBSD/patches/2.9/common/024\\_sshafs.patch](ftp://ftp.openbsd.org/pub/OpenBSD/patches/2.9/common/024_sshafs.patch)  
[ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.0/common/019\\_sshafs.patch](ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.0/common/019_sshafs.patch)