

# [UNIX] KisMAC Local Privilege Escalation

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-09/0021.html>

---

**From:** SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

**Date:** 09/07/03

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 7 Sep 2003 18:23:46 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

-----

KisMAC Local Privilege Escalation

---

## SUMMARY

KisMAC is a popular wireless network identification and analysis tool. In the event that the "SUID Shell Scripts are enabled" checkbox (inside of the driver tab under preferences) is enabled, an attacker with local interactive access can become root through several different mechanisms. This feature is off by default.

## DETAILS

@stake has identified five potential vulnerabilities within the setuid shell scripts enabled by KisMAC. The core issue is that an attacker can cause these shell scripts to use an attacker-controlled directory instead of a system directory by hardlinking to any of the vulnerable shell scripts. This happens during the execution of `dirname(1)`.

`viha_driver.sh / macjack_load.sh / airojack_load.sh`

1) Change the ownership of user controlled files. Since we can change the value of `$DRIVER_KEXT`, we can cause the `chown` command within the `load_driver` function to change the ownership of a file/directory of our choosing. An attacker can create a setuid executable owned by the attacker's uid, that will get `chown()`'d to root. While the example used is the `viha_driver.sh` script, both `macjack_load.sh` and `airojack_load.sh` can

## Securiteam: [UNIX] KisMAC Local Privilege Escalation

also be used.

2) Load arbitrary kernel modules. The line underneath the chown show the loading of the kernel extension located in \$DRIVER\_KEXT. Since we can control this value, we can cause arbitrary kernel modules of our choosing to be loaded into memory. While the example used is the viha\_driver.sh script, the macjack\_load.sh and airojack\_load.sh scripts can also be used.

exchangeKernel.sh

3) Install arbitrary kernel. Using similar techniques outlined above, an attacker can overwrite the kernel with a kernel of their choosing.

setuid\_enable.sh / setuid\_disable.sh

4) Change the ownership of user controlled files. Both setuid\_enable.sh and setuid\_disable.sh script are vulnerable to the attack outlined in vulnerability #1. Additionally, setuid\_enable.sh will actually add the setuid bit to user controlled files after chown()ing the files to root.

viha\_prep.sh / viha\_unprep.sh

5) Execution of attacker controlled binary. Using a technique similar to vulnerability #1, an attacker can cause an executable of their choosing to be executed as root.

Vendor Response:

Upgrade to 0.05d4 at:

<<http://www.binaervarianz.de/projekte/programmieren/kismac/download.php>>  
<http://www.binaervarianz.de/projekte/programmieren/kismac/download.php>.

Recommendation:

Do not enable this functionality on a multi-user machine. If this is a requirement, only allow users with in the admin group access to the setuid shell scripts.

### ADDITIONAL INFORMATION

The original advisory can be downloaded from:

<<http://www.atstake.com/research/advisories/2003/a082203-1.txt>>  
<http://www.atstake.com/research/advisories/2003/a082203-1.txt>.

The information has been provided by <<mailto:daveg@atstake.com>> Dave G. of @Stake.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:  
[list-unsubscribe@securiteam.com](mailto:list-unsubscribe@securiteam.com)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto:list-subscribe@securiteam.com)

=====

=====

## Securiteam: [UNIX] KisMAC Local Privilege Escalation

### DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.