

# [NT] My Firewall Plus Privilege Escalation Vulnerability

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-12/0066.html>

---

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

**Date:** 12/21/04

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

Date: 21 Dec 2004 18:03:12 +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>

-----

My Firewall Plus Privilege Escalation Vulnerability

---

## SUMMARY

<<http://www.webroot.com/products/myfirewallplus/>> My Firewall Plus is a "Corporate strength firewall for your personal PC".

Secunia Research has discovered a vulnerability in My Firewall Plus, which can be exploited by malicious, local users to gain escalated privileges.

## DETAILS

Vulnerable Systems:

\* My Firewall Plus version 5.0 (build 1117)

The vulnerability is caused due to the "Smc.exe" process invoking the help functionality with SYSTEM privileges.

This can be exploited to execute arbitrary programs on a system with escalated privileges.

Solution:

Apply patch: <[http://www.webroot.com/services/MFP\\_Patch.exe](http://www.webroot.com/services/MFP_Patch.exe)>

Securiteam: [NT] My Firewall Plus Privilege Escalation Vulnerability

[http://www.webroot.com/services/MFP\\_Patch.exe](http://www.webroot.com/services/MFP_Patch.exe)

Time Table:

- 15/11/2004 – Vulnerability discovered.
- 15/11/2004 – Vendor notified.
- 15/11/2004 – Vendor response.
- 16/12/2004 – Vendor issues patch.
- 21/12/2004 – Public disclosure.

ADDITIONAL INFORMATION

The information has been provided by <mailto:che@secunia.com> Carsten H. Eiram.

The original article can be found at:

<[http://secunia.com/secunia\\_research/2004-16/](http://secunia.com/secunia_research/2004-16/)>  
[http://secunia.com/secunia\\_research/2004-16/](http://secunia.com/secunia_research/2004-16/)

=====

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

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====  
=====

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.