

# [NT] Norton Antivirus Corporate Edition Privilege Escalation

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-10/0126.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 10/25/02

From: [support@securiteam.com](mailto:support@securiteam.com)

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

Date: 25 Oct 2002 15:14:34 +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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

-----

Norton Antivirus Corporate Edition Privilege Escalation

---

## SUMMARY

A security vulnerability in Norton Antivirus allows local attackers to run winhlp32 in context of local system. This would allow them to gain elevated privileges.

## DETAILS

Vulnerable systems:

\* Norton Antivirus Corporate Edition version 7.60 Build 962

\* Norton Antivirus Corporate Edition version 7.5.1 Build 62

\* Norton Antivirus Corporate Edition version 7.6.1 Build 35a

Norton Antivirus adds "Scan for Viruses..." item to Explorer's context menu. Application launched if this item is selected has local system context. Application has "Help" button which allows starting winhlp32 in context of Local System. Winhlp32 allows user to execute code with credentials of this application.

Vendor response:

According to Symantec reply on the moment this problem was reported to Symantec fix was ready and tested:

Securiteam: [NT] Norton Antivirus Corporate Edition Privilege Escalation

This vulnerability has been eliminated in current versions of Symantec Norton Antivirus Corporate Edition, version 7.5.1 Build 62 and later as well as version 7.6.1 Build 35a and later that are available for download.

ADDITIONAL INFORMATION

The information has been provided by <mailto:[3APA3A@SECURITY.NNOV.RU](mailto:3APA3A@SECURITY.NNOV.RU)>  
3APA3A.

This issue was discovered by ERRor of Domain Hell Team.

=====

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)

=====

=====

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.

- 
- **Previous message:** [support@securiteam.com](mailto:support@securiteam.com): "[UNIX] XSS Vulnerability in Mojo Mail Sign-Up Form"
  - **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)