

[NT] Norton Insufficient Validation of Driver Input Buffer (SymEvent)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-09/msg00024.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxxx>
 - *Date:* 19 Sep 2006 17:39:48 +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>

Norton Insufficient Validation of Driver Input Buffer (SymEvent)

SUMMARY

Norton Personal Firewall is a desktop firewall application produced by <http://www.symantec.com/> Symantec.

Norton Personal Firewall crashes when arbitrary data is sent to its SymEvent driver.

DETAILS

Vulnerable Systems:

- * Norton Personal Firewall 2006 version 9.1.0.33
- * probably all versions of Norton Personal Firewall 2006 and Norton Internet Security 2006
- * possibly older versions of Norton Personal Firewall and Norton Internet Security

Norton insufficiently protects its driver '\Device\SymEvent' against a manipulation by malicious applications and it fails to validate its input buffer. It is possible to open this driver and send arbitrary data to it, which are implicitly believed to be valid. It is possible to assemble the

[NT] Norton Insufficient Validation of Driver Input Buffer (SymEvent)

data in the input buffer such that the driver performs an invalid memory operation and crashes the whole operating system. Further impacts of this bug were not examined.

Proof of concept:

<<http://www.matousec.com/downloads/windows-personal-firewall-analysis/BTP00011P002NF.zip>>
<http://www.matousec.com/downloads/windows-personal-firewall-analysis/BTP00011P002NF.zip>

Disclosure Timeline:

- * 2006-09-16 – Vulnerability confirmed by popular information sources
- * 2006-09-15 – Advisory released
- * 2006-09-15 – Vendor notification

ADDITIONAL INFORMATION

The information has been provided by Matousec.

The original article can be found at:

<<http://www.matousec.com/info/advisories/Norton-Insufficient-validation-of-SymEvent-driver-input-buffer.php>>
<http://www.matousec.com/info/advisories/Norton-Insufficient-validation-of-SymEvent-driver-input-buffer.php>

=====

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@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====
=====

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.