

# [NT] Orenosv HTTP/FTP Server Multiple Buffer Overflows

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-05/0072.html>

---

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

**Date:** 05/10/05

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

Date: 10 May 2005 13:12:11 +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>

-----

Orenosv HTTP/FTP Server Multiple Buffer Overflows

---

## SUMMARY

" <[http://hp.vector.co.jp/authors/VA027031/orenosv/index\\_en.html](http://hp.vector.co.jp/authors/VA027031/orenosv/index_en.html)> Orenosv is a stable, reliable and efficient HTTP/FTP/FTPS server that can operate 24H/365D. Orenosp runs on Windows platforms (NT, 2000, XP and 2003) and Linux x86."

Mutiple buffer overflows vulnerabilities were found in Orenosv's server.

## DETAILS

Vulnerable Systems:

\* Orenosv HTTP/FTP Server version 0.8.1

Immune Systems:

\* Orenosv HTTP/FTP Server version 0.8.1a

Multiple FTP Commands Buffer Overflow Vulnerability:

These buffer overflow is triggered when the server receives a FTP file/directory manipulation command with a filename that is 249 or 250 bytes long.

## Securiteam: [NT] Orenosv HTTP/FTP Server Multiple Buffer Overflows

For 4-character FTP file/directory commands, 249-bytes filenames will cause the overflow. Examples of 4-character FTP commands include LIST, DELE, RETR etc.

For 3-character FTP commands, 250-bytes filenames will cause the overflow. 3-character FTP commands include MKD, RMD, CWD, etc.

The server restricts the maximum length of each input line, hence using a filename that is longer than 250 will not trigger the vulnerable function.

Reverse engineering the orenosv.exe file reveals that the problem lies in the unbounded copy that occurs within the ftp\_xlate\_path(), ftp\_is\_canonial() and os\_fn\_nativize() functions, as well as due to several unsafe use of sprintf().

Exploitation is complicated by the fact that the buffer is limited to 250 bytes.

Orenosv runs in two separate processes.

- (1) The monitoring process
- (2) The server process

The monitoring process will restart the server process if it crashes due to the overflow. On our test system, we were able to cause a DoS on the server by sending the overflow buffer in quick successions to the server. This causes both the server and monitor process to crash, thus preventing any automatic restart.

Long SSI Command Buffer Overflow Vulnerability (cgissi.exe):  
Orenosv supports the use of SSI (.shtml). This supported is provided by cgissi.exe. A buffer overflow vulnerability exists in cgissi.exe when processing an overly long SSI command name. The overflow occurs in the parse\_cmd() function. In this function, a loop performs an unsafe copy of the SSI command name to a local stack buffer. This copy loop is terminated by the space character. Exploitation may be limited since the SSI command name is limited to less than 128 bytes.

Disclosure Timeline:

- \* 26.04.05 – Vulnerability Discovered
- \* 28.04.05 – Initial Author Notification
- \* 29.04.05 – Initial Author Reply
- \* 01.05.05 – Author Provided Fix for Testing
- \* 01.05.05 – Informed Author that Overflow will still occur in os\_fn\_nativize()
- \* 01.05.05 – Author Provided Another Fix for Testing
- \* 01.05.05 – Informed Author that Overflow will still occur due to several unsafe sprintf()
- \* 05.05.05 – Author Provided Another Fix for Testing
- \* 05.05.05 – Informed Author of Potential Problem in STOU command
- \* 06.05.05 – Author Provided Auother Fix for Testing
- \* 07.05.05 – Author Released Patch

Securiteam: [NT] Orenosv HTTP/FTP Server Multiple Buffer Overflows

\* 08.05.05 – Public Release

ADDITIONAL INFORMATION

The information has been provided by <mailto:chewkeong@security.org.sg>  
Chew Keong TAN.

The original article can be found at:

<<http://www.security.org.sg/vuln/orenosv081.html>>

<http://www.security.org.sg/vuln/orenosv081.html>

=====

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.