

# [REVS] Microsoft PCT Exploit Analysis

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-10/0006.html>

---

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

**Date:** 10/04/04

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

Date: 4 Oct 2004 13:52:18 +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>

-----

Microsoft PCT Exploit Analysis

---

## SUMMARY

The paper linked below provides an extensive analysis to the Microsoft PCT Vulnerability patched in MS04-011. David Schulhoff's paper focuses on <http://www.securiteam.com/windowsntfocus/5CP0L0KCKO.html> > THC's exploit, and provides an excellent tutorial on exploits in general, with thorough examples.

## DETAILS

Abstract:

On the second Tuesday, what many now refer to as patch Tuesday , of April, 2004, Microsoft released four security bulletins. Among these was <http://www.microsoft.com/technet/security/bulletin/MS04-011.msp> > Microsoft Security Bulletin MS04-011 which detailed fourteen separate vulnerabilities, six of them rated critical for one or more Windows operating systems. In the list of the vulnerability identifiers in the Technical Details section of the bulletin is the PCT Vulnerability which is also referenced as CAN-2003-07191 on the Common Vulnerabilities and Exposures website. PCT is referred to variously within Security Bulletin MS04-011 as the Private Communications Transport or Private Communication Technology protocol. For the purposes of this paper David Schulhoff selected this vulnerability and a corresponding exploit to examine in

Securiteam: [REVS] Microsoft PCT Exploit Analysis

detail. We will take a look at both what makes this vulnerability a classic opportunity for exploitation and how its unique characteristics provide an insight into some basic security principles. David Schulhoff takes the approach of an individual seeking to take advantage of this opportunity , and then look at two different scenarios of organizations dealing with an incident caused by an attack on the PCT vulnerability.

ADDITIONAL INFORMATION

The whitepaper can be found at:

<[http://www.thc.org/root/docs/exploit\\_analysis/SSL\\_PCT\\_EXPLOITATION\\_ANALYSIS.PDF](http://www.thc.org/root/docs/exploit_analysis/SSL_PCT_EXPLOITATION_ANALYSIS.PDF)>  
[http://www.thc.org/root/docs/exploit\\_analysis/SSL\\_PCT\\_EXPLOITATION\\_ANALYSIS.PDF](http://www.thc.org/root/docs/exploit_analysis/SSL_PCT_EXPLOITATION_ANALYSIS.PDF)

=====

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.