

# [NT] Intellisol XPede Exposes Passwords

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-03/0098.html>

---

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

*Date:* 03/23/02

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

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

Date: Sat, 23 Mar 2002 17:38:01 +0100 (CET)

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.

-----

Intellisol XPede Exposes Passwords

---

## SUMMARY

<<http://www.workforceroi.com/solutions/pa/index.shtml>> Intellisol XPede is a browser-based time and expense entry and project cost management module designed to connect a remote workforce on a real-time basis. Intellisol Project Accounting is designed for any professional service organization such as consulting, software development, law, architecture, engineering, PR/advertising and more with between 10 and 500 million dollars in revenue and up to 500 employees, and integrates with Microsoft Great Plains Business Solutions financial suites. Two security vulnerabilities has been discovered in the way XPede handle users' passwords.

## DETAILS

Vulnerable systems:

XPede version 4.1

XPede version 7.x series

Vulnerability #1:

XPede's cookies store users password "ciphered" in a very weak manner (a mix of shifts and permutations), recovering a clear text password from there is really trivial making users remotely vulnerable from cross site scripting based attacks, various MSIE bugs while users are locally



Securiteam: [NT] Intellisol XPede Exposes Passwords

[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): "[NT] Automatically Opening Internet Explorer and Execution of Attachments (WebBrowser)"
- *Messages sorted by:* [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)