

[NEWS] PureTLS Gets a Security Upgrade

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-03/0043.html>

From: support@securiteam.com

Date: 03/09/02

From: support@securiteam.com

To: list@securiteam.com

Date: Sat, 9 Mar 2002 12:35:28 +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.

PureTLS Gets a Security Upgrade

SUMMARY

<<http://www.rtfm.com/puretls/>> PureTLS is a free Java-only implementation of the SSLv3 and TLSv1 (RFC2246) protocols. Multiple security vulnerabilities in the product have been found during a code audit. A new version is now available to fix these.

DETAILS

Internal audits prior to the release of PureTLS 0.9b2 discovered a potential attack under certain conditions. This vulnerability was present in all prior versions. Details of this vulnerability have not been disclosed and are being withheld now to allow users time to upgrade. As far as we know, this attack has not been exploited in the wild and is not publicly known.

All users of older versions are strongly urged to upgrade immediately. The new version can be downloaded from: <<http://www.rtfm.com/puretls>>
<http://www.rtfm.com/puretls>

ADDITIONAL INFORMATION

The information has been provided by <<mailto:ekr@rtfm.com>> Eric Rescorla.

Securiteam: [NEWS] PureTLS Gets a Security Upgrade

=====
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.

- **Previous message:** support@securiteam.com: "[EXPL] MTR Allows Local Users to Gain Root Privileges"
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)