

[NT] PlatinumFTPserver Format String Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-12/0080.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 12/23/03

To: list@securiteam.com

Date: 23 Dec 2003 20:05:48 +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>

PlatinumFTPserver Format String Vulnerabilities

SUMMARY

<<http://www.platinumftp.com/platinumftpserver.html>> PlatinumFTPserver "simplifies management of all your FTP clients with regards to sending and receiving program and data files over an IP connection". A vulnerability in the product allows remote attackers to supply formatting strings to the FTP server. This would allow them to cause the server to execute arbitrary code.

DETAILS

Vulnerable systems:

* PlatinumFTPserver version 1.0.18

A remote user can supply a specially formatted command to trigger a format string flaw in PlatinumFTPserver and potentially execute arbitrary code.

Some vulnerable commands are provided:

user %s%s%s%s

mkdir %s%s%s%s

rename filename %s%s%s%s

Securiteam: [NT] PlatinumFTPserver Format String Vulnerabilities

ADDITIONAL INFORMATION

The information has been provided by Jan-Olivier Filiols and Philippe Oechslin.

=====

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.