

[NEWS] Spectrum Cash Receipting System Weak Password Encryption

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-01/0125.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 01/26/05

To: list@securiteam.com

Date: 26 Jan 2005 18:59:47 +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>

Spectrum Cash Receipting System Weak Password Encryption

SUMMARY

The Spectrum Cash Receipting System is a client/server software solution that allows offline work, and thus offline authentication. The application has several layers of authority with regards to authorizing payments.

The local authentication requires the password file for the application to reside locally.

Portcullis discovered that Spectrum's mechanism for protecting the passwords within the password file is a static substitution algorithm. Additional properties of the system reduce the available key-space, expose plaintext in the ciphertext, enforce a maximum password length and reveal the length of the password in the password file.

DETAILS

Vulnerable Systems:

* Spectrum Cash Receipting System version 6.406.8

Having the password file locally allows an attacker to enumerate valid

Securiteam: [NEWS] Spectrum Cash Receipting System Weak Password Encryption

users on the system and potentially gain unauthorized access to the system through brute force attempts on those valid user's passwords. Furthermore valid users of the system could attempt privilege escalation as they have full details of all valid user accounts.

When creating a password in the application the algorithm converts all letters entered to lowercase and limits the length to a maximum of 6 characters. In the substitution stage it statically substitutes alphanumeric characters with a character from the range a-z and the special characters "@+&()?\|<>". Any character in the password that is not alphanumeric is not substituted and becomes part of the ciphertext. If the password is shorter than 6 characters the algorithm pads the ciphertext with white-space accordingly.

Impact:

The impact of this vulnerability is that an attacker with local access to the password file can retrieve the plaintext passwords of all the system users.

ADDITIONAL INFORMATION

The information has been provided by <mailto:PJD@portcullis-security.com>
Paul J Docherty.

=====

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.