

[NEWS] Predictability and Vulnerability in the Canadian Firearms Centre's On-Line Services Web Site

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-09/0043.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 09/16/03

To: list@securiteam.com

Date: 16 Sep 2003 15:33:30 +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>

Predictability and Vulnerability in the Canadian Firearms Centre's On-Line Services Web Site

SUMMARY

The <<http://www.cfc-ccaf.gc.ca/>> Canadian Firearms Centre (CFC) is the Canadian Government's department responsible for implementing Gun Control regulations in Canada.

On their On-Line Services site, users may register non-restricted firearms, re-register restricted and prohibited firearms, check the status of their license application, check the status of their firearm registration application, and change their mailing and/or residential address.

Two related security issues allow a malicious user to not only test and extract valid/invalid License Numbers, but also brute-force accounts. However, it is only realistically feasible on accounts that have been secured using a Personal Identification Number (PIN).

A third security issue allows a malicious user wishing to target an individual, where personal information is available, but the intended

account to protected by a PIN, to force the PIN to be reset without contacting any support personnel and making such a request.

DETAILS

Information Extraction

The site uses a 2-stage method for requesting a client's License Number. Upon entering a valid License Number, users are presented with either a request for personal information, or a request for a PIN number. Upon entering an invalid License Number, users are presented with a screen stating the "License/FAC number is invalid. Correct format is first 8 digits of License or last 7 digits of FAC number as it appears on your card."

Since there is no protection against brute-forcing, it would be trivial for a malicious user to create an application to sequentially enter License Numbers, and therefore determine, not only what range of numbers are used, but also which precise License Numbers have been issued.

The site designers have included a hidden form field in order to track how many guesses have been made, but at no time is this form field ever modified, therefore invalidating its use. The hidden field looks like this: `<input type="hidden" name="logonAttempts" value="1">`

Brute-Forcing of PIN-protected Accounts

Once a malicious user has determined which number sequences match valid License Numbers, they are presented with either a screen requesting personal information, or a screen requesting the client's PIN. The screen requesting personal information is the default, with users able to establish a PIN to allow easier logins.

The site designers once again included a hidden form field that looks like this: `<input type="hidden" name="logonAttempts" value="1">`. Despite the fact that this hidden form field is tracked by the application, it is subject to tampering because the application blindly trusts the number in the field. For example, entering a value such as `<input type="hidden" name="logonAttempts" value="-999999">` produces a returned hidden form field of `<input type="hidden" name="logonAttempts" value="-999998">` thus giving a malicious user as many attempts as they like.

To make it even easier to create a brute-forcing program, any non-numeric value forces the application to reset the hidden form field to `<input type="hidden" name="logonAttempts" value="1">`. Therefore, instead of issuing a number great enough to guess the PIN before reaching the maximum 3 attempts, all a malicious program has to do is issue a non-numeric value to enable unlimited PIN guessing attempts.

Three (3) Invalid PINs Forces Reset

Upon submitting three (3) invalid PIN numbers, the system automatically resets account access to the client's personal information. This would allow a malicious person to target any individual for whom they have

sufficient personal information, but where a PIN has been used to protect the account. Furthermore, creating an application to identify each valid License Number as well as resetting client PINs would be a trivial process.

Solution(s):

The easiest solution from the end-users point of view is to choose not to protect their account with a PIN, therefore requiring either personal knowledge of and individual and their correct License Number or brute-forcing of 3 separate pieces of personal information (Last Name, Date of Birth, and Place of Birth), which would be highly labor intensive as well as highly prone to failure.

However, a notice recently added to the web site states "In future access to services on this site may be limited to clients with a PIN." making the brute-forcing vulnerability much more serious.

Finally, always protect your personal information in order to prevent Identity Theft.

Vendor status:

25MAR2002 – CFC Management was originally notified of this vulnerability.

12FEB2003 – The issue was raised again with CFC Management on, when the Web Site was re-launched without correcting the outstanding issues.

18AUG2003 – The CFC was notified under the terms of Full Disclosure Policy (RFPolicy) V2.0

25AUG2003 – No reply had been received, but due to the State of Emergency because of massive blackouts in the province of Ontario, the researcher decided to extend the requirement for initial response by 5 days.

05SEP2003 – No reply had been received, so a second email communication was sent to the CFC. The email gave 12 September 2003 as a deadline to receive a reply. This email is confirmed to have been read by both the CEO, Bill Baker, and by the Communications Secretary.

10SEP2003 – The CFC's Manager of Informatics replied to the advisory at the request of William Baker, Commissioner of the Canada Firearms Centre. In his reply, he stated: "matters raised in your correspondence have previously been examined by the centre, as part of its ongoing security reviews. Currently, our system meets the Government of Canada standards for the data available through our Internet site", however no details as to when, or by whom, these 'security reviews' were conducted, nor any details as to which 'standards' are referred to. As of the date of his email, none of the above vulnerabilities have been corrected.

15SEP2003 – Public release of this advisory.

ADDITIONAL INFORMATION

The information has been provided by <mailto:john@jjhicks.com> John Hicks.

=====

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.