

[NT] Safeboot PC Security User Emuneration Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-03/0075.html>

From: support@securiteam.com

Date: 03/23/03

From: support@securiteam.com

To: list@securiteam.com

Date: 23 Mar 2003 18:30:05 +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

In the US?

Contact Beyond Security at our new California office housewarming rates on automated network vulnerability scanning. We also welcome ISPs and other resellers!

Please contact us at: 323-882-8286 or ussales@beyondsecurity.com

Safeboot PC Security User Emuneration Vulnerability

SUMMARY

Safe boot PC security allows the discovery (by trial and error) of valid user account names by distinguishing between bad login names and bad passwords.

DETAILS

Vulnerable systems:

- * Safeboot version 4.1 (current version)

Safeboot (www.safeboot.com) is a software product to prevent access to a PCs hard disk drive. This protection takes two forms:

- 1) Pre-Boot user authentication,
- 2) Hard Disk Encryption. It is with the former that IRM identified a vulnerability.

Securiteam: [NT] Safeboot PC Security User Emuneration Vulnerability

Whilst Safeboot supports a number of hardware-based tokens to provide user authentication, without these it relies on Username and Password Authentication.

When a user has entered a bad username or password, Safeboot will produce an error, specifically stating which of the credentials (username or password) is incorrect. By leaving the password blank or entering anything, an attacker could use trial and error to establish valid usernames for this or other related systems, before proceeding to attempt discovery of the associated password.

Vendor & Patch Information:

The vendor of this product, Control Break International, was contacted. They were receptive to our report and produced a statement reproduced here:

"Control Break International is aware of IRM's findings. We have not considered enumeration of the user list sensitive information up to now, as real-world user ID's are often trivial combinations of first name, last name, and initials, and are usually easily guessable through social engineering. With the popularity of directory systems such as AD and Novell, user id's are increasingly similar to e-mail addresses, yielding them even simpler to determine. We are however sensitive to customer concerns, so for those who would like to redefine the error messages reported for incorrect user id and password information, we can make available replacement error message files accordingly".

These error message files are not available for public download, but users of Safeboot can obtain it by contacting Control Break via their Website.

Workarounds:

See Vendor and Patch Information.

ADDITIONAL INFORMATION

The information has been provided by <mailto:advisories@irmplc.com> IRM Security Advisory.

=====

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,

Securiteam: [NT] Safeboot PC Security User Emuneration Vulnerability

loss of business profits or special damages.