Vulnerability Note VU#900031

Faircom c-treeACE database weak obfuscation algorithm vulnerability

Original Release date: 10 Jun 2013 | Last revised: 11 Jun 2013

Overview

Faircom c-treeACE provides a weak obfuscation algorithm (CWE-327) that may be unobfuscated without knowledge of a key or password. The algorithm was formerly called Faircom Standard Encryption but is now called Data Camouflage.

Description

Faircom c-treeACE provides a weak obfuscation algorithm that may be unobfuscated without knowledge of a key or password. Faircom formerly described this algorithm as follows:

> *FairCom Standard Encryption*
>
> *Using our standard proprietary encryption algorithm provides the means to add an extra level of confidentiality to an application's data. FairCom designed its proprietary encryption algorithm for speed and efficiency, focusing on minimizing performance loss.*
> *The encryption algorithm is proprietary to FairCom Corporation and the details are not released in any way to increase the difficulty of reverse-engineering the process. While reverse-engineering is a violation of the licensing agreement, it remains a remote possibility, and FairCom does everything possible to limit the potential exposure of the FairCom algorithms.*
> *This Standard File Encryption is not intended as a replacement for OS or other security systems, however, as a supplement to existing security. Standard File Encryption is suitable for most needs with excellent security vs. performance tradeoffs.*

Faircom has come up with a new branding called "Data Camouflage" so it will be less likely to be confused with standard encryption algorithms, such as, AES. Faircom describes the "Data Camouflage" algorithm as follows:

> *Data Camouflage*
>
> *Using our Data Camouflage technique provides the means to add an extra level of confidentiality to an application's data. FairCom designed this approach to mask the file on the disk without sacrificing speed and efficiency, focusing on minimizing performance loss.*
>
> *Data Camouflage is not intended as a replacement for OS or other security systems, however, as a supplement to existing security. It is suitable for most needs with excellent security vs. performance tradeoffs. With this approach, you can protect data on disk from unauthorized inspection, but any c-treeACE client can access the protected files. To avoid this, the Advanced File Encryption option includes the ability to have hidden keys. Proper implementation of user access controls within c-treeACE is also recommend to prevent unauthorized access to data, even it not masked with the Data Camouflage feature.*

An attacker that is able to obtain a c-treeACE database that is obfuscated using the Data Camouflage algorithm (formerly Faircom Standard Encryption) may be able to unobfuscate the database by moving it to a trial install of c-treeACE, deleting the .fcs configuration files and replacing the .fcs files with the default files from the trial. This will allow the attacker to authenticate to the database with default ADMIN/ADMIN credentials and view the contents of the obfuscated database.

Impact

An attacker that is able to obtain a database that uses the Data Camouflage algorithm (formerly Faircom Standard Encryption) may be able to unobfuscate the contents of the database.

Solution

Use Faircom's Advanced File Encryption

To ensure the confidentiality of the database contents, the Advanced File Encryption algorithm should be used. Faircom's Advanced File Encryption provides standard encryption algorithms such as AES.

Vendor Information (Learn More)

Vendor	Status	Date Notified	Date Updated
Faircom	Affected	25 Apr 2013	20 May 2013
Henry Schein	Affected	10 Jun 2013	11 Jun 2013

If you are a vendor and your product is affected, let us know.

CVSS Metrics (Learn More)

Group	Score	Vector
Base	6.0	AV:L/AC:M/Au:S/C:C/I:C/A:N
Temporal	5.7	E:ND/RL:W/RC:C
Environmental	4.3	CDP:ND/TD:M/CR:ND/IR:ND/AR:ND

References

- http://cwe.mitre.org/data/definitions/327.html
- http://www.faircom.com/doc/ctreeplus/index.htm#29876.htm
- http://www.faircom.com/doc/ctreeplus/index.htm#30280.htm
- http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Credit

Thanks to Justin Shafer for reporting this vulnerability.

This document was written by Jared Allar.

Other Information

CVE IDs: CVE-2013-0148

Date Public: 10 Jun 2013

Date First Published: 10 Jun 2013

Date Last Updated: 11 Jun 2013

Document Revision: 25

Feedback

If you have feedback, comments, or additional information about this vulnerability, please send us email.