By Date By Thread

List Archive Search

ARA-2020-005: Insecure Direct Object Reference in 1CRM (CVE-2020-15958)

From: Andreas Sperber <andreas.sperber () aramido de>
Date: Mon, 14 Sep 2020 15:05:52 +0200

~~~~
# Security Advisory
ARA-2020-005: Insecure Direct Object Reference (CVE-2020-15958)
## Affected Product(s) and Environment(s)
Product: 1CRM <=8.6.7, confirmed for CRBM System ENT-8.6.5, CRBM System
ENT-8.6.6 and Startup+ Edition 8.5.15
Environments: All host environments
## Security Risk
Severity: High
CVSS v3: 8.6
## Impact
Confidentiality: High
Integrity: None
Availability: None
## Exploitability
Access Vector: Network
Access Complexity: Low
Privileges Required: None
User Interaction: None
## Scope
Scope: Changed
## Weakness Classification
[CWE-862](https://cwe.mitre.org/data/definitions/862.html): Missing
Authorization
[CWE-219](https://cwe.mitre.org/data/definitions/219.html): Storage of
File with Sensitive Data Under Web Root
[CVE-2020-15958](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15958)
## Remediation Level
Sensitive files must not be stored within the web root or below. These
files should be stored in a folder outside the web root and secured
accordingly. A proper access control must be established to deliver
these files to authorized users only.
## Timeline
*2020-07-27: Preliminary CVE Assignment by MITRE
*2020-07-27: Vendor notification
*2020-07-28: Notification of vendor's master partner for Germany
Visual4, as requested by vendor
*2020-07-31: Visual4 acknowledges vulnerability
*2020-08-14: Visual4 issues security alert for all 1CRM on-premise
systems and requests immediate update to version 8.6.7 [1]
*2020-08-20: Visual4 informs customers by mail about security alert
*2020-08-27: Vendor reports fix of vulnerability to aramido; fix could
not yet be verified, public documentation not sufficient
*2020-09-14: Public disclosure after 45 days of initial vendor notification
## Description Summary
1CRM stores uploaded and other files within its web root. Due to
incomplete authorization checks, an unauthenticated user can remotely
access these files. Although filenames must be known, 1CRM follows a
well-known naming pattern for at least some sensitive files.
## Product Introduction
"The all-in-one CRM solution for managing every aspect of your business
online. Collaborate effectively with your team, from near and far.
1CRM provides everything you need to manage your business online. Start
with a complete CRM solution including lead forms and eCommerce
integration. Add a portal to connect with your customers and provide
self-service options including appointment scheduling. Top things off
with a sophisticated marketing automation platform to help turn your
leads into customers!"
*Source:*[1CRM Website](https://1crm.com/)
## Technical Description
1CRM allows to upload files on several occasions, e.g. to record
*Expenses*and *Purchase Orders*, add personal information to
*Accounts*and *Contacts*, and to manage *Human Resources*by adding CVs
and so on. Additionally, backups can be created manually or via a cron
job alike automatism. Backups can be configured to include the database,
application configs, file attachments and modules.
All those files are stored in folders within the root directory of the
web server (web root). A download script *download.php*exists, which is
to ensure authorized access to the files. If a user is not authenticated
or has not enough permissions, the error "Authentication required" is
displayed.
Example:
[/download.php?type=DocumentRevisions&id=69cabcb5-c909-2379-9c8a-5f187453fab1&ver=88f87&field=filename](/download.php?
type=DocumentRevisions&id=69cabcb5-c909-2379-9c8a-5f187453fab1&ver=88f87&field=filename)
However, it is also possible to access the files stored in the web root
via an insecure direct object reference. As a matter of fact, the
application makes use of this way of access to download
*Expense*attachments and backups (and not via the regular download.php
script). The request on such a file is not handled by the 1CRM
application but answered by the web server itself. As the folders are
not protected in any special way, the files are accessible to anyone.
It is necessary for such a request to know the URI. 1CRM implements a
predictable folder structure such as
[/files/upload/42/](/files/upload/42/) and some of the most sensitive
files have a predictable, at least guessable name such as
[backup_20380119_031407.zip](backup_20380119_031407.zip).
### Proof of Concept (PoC)
A backup file, which might contain all the CRM's information including
clear text passwords of linked mailboxes, is stored in
[/files/backups/](/files/backups/). The file contains the date and the
time the archive was created. Assuming the backup is created on a daily
bases, guessing the date is trivial. Guessing the time could be achieved
by trying out all 86.400 possibilities. However, creating backups
usually during nightly hours narrows this number further down.
The backup is an unencrypted file and can for example be access via
[/files/backups/backup_20380119_031407.zip](/files/backups/backup_20380119_031407.zip).
Other uploaded files are stored under
[/files/upload/\<id>/](/files/upload/<id>/). While it is not a big
challenge to guess the \<id>-part, it is harder to determine the actual
filenames. These filenames are generated by the user and not at random.
Assuming a sales man names an offer according to a certain scheme, e.g.
Offer_20380119-1.pdf, it might be tempting to try similar names. If this
vulnerability is combined with another weakness, such as a directory
listing, an adversary would be able to easily obtain all exposed files.
## Solution
We strongly recommend to store sensitive data outside the web root. By
this, an adversary cannot directly access those file but a download
mechanism must be implemented. This download script, which already
exists, must ensure the authorization of the requester.
As an urgent solution we recommend 1CRM hosters to place an .htaccess
file within the affected folders. The .htaccess file must contain the
following for an Apache setup:
```

Order deny,allow
~~~~

Deny from all
```

Furthermore, we suggest to use random file names when storing them into a file system. The real file name can be stored into the database if necessary. A random file name can be chosen in a way to be hardly guessable and to only use secure characters for any operating or file system.
Due to the big impact in case a backup file was leaked, we suggest to always encrypt backup files.
Upon fix of all findings by the vendor, we suggest on premise hosters the update to the most recent version (at least 8.6.7). Additional security measurements such as segmentation and the usage of a virutal private network (VPN) are strongly advised.

References

[0][aramido responsible disclosure policy](https://aramido.de/blog/Sicherheitshinweise)
[1][Die Sicherheit Ihres CRM-Systems auf maximale Stufe drehen](https://1crm-system.de/crm-ratgeber/sicherheit-webanwendungen/)
[2][Sicherheitswarnung: 1CRM schützt Daten unzureichend (CVE-2020-15958)](https://aramido.de/blog/sicherheitshinweise/sicherheitswarnung-1crm-schutzt-daten-unzureichend-cve-2020-15958)

Authors

Christoph Biedl, aramido GmbH
E-mail: christoph.biedl () aramido.de
PGP-Key: https://aramido.de/christoph.biedl.asc
PGP-Fingerprint: 04DF BDFD 81D4 4537 FF20 A8A5 C73C F15B 3780 F158
Andreas Sperber, aramido GmbH
E-mail: andreas.sperber () aramido.de
PGP-Key: https://aramido.de/andreas.sperber.asc
PGP-Fingerprint: FC84 BB4D 696D F04C E1A1 2BED 7518 A24A 06B9 BEA7

aramido - Information Security Consultancy

aramido is a trusted consultancy for information security from Karlsruhe. aramido advises companies and other organizations on information security issues, checks systems, for example, through penetration tests, and helps with security incidents through a rapid incident response.

aramido GmbH
Amalienstraße 24
76133 Karlsruhe, Germany
Management board: Armin Harbrecht, Andreas Sperber
Web: https://aramido.de

Disclaimer

The information provided in this advisory is provided "as is" without any warranty. Details of this security advisory may be updated in order to provide as accurate information as possible. The latest version of this security advisory is available on the aramido web site. aramido GmbH disclaims all warranties, either expressed or implied, including the warranties of merchantability and capability for a particular purpose. aramido GmbH or its suppliers are not liable in any case of damage, including direct, indirect, incidental, consequential loss of business profits or special damages, even if aramido GmbH or its suppliers have been advised of the possibility of such damages. Some states do not allow the exclusion or limitation of liability for consequential or incidental damages so the foregoing limitation may not apply. We do not approve or encourage anybody to break any vendor licenses, policies, deface websites, hack into databases or trade with fraud/stolen material.

Copyright

Attachment: **signature.asc**
Description: OpenPGP digital signature

By Date By Thread

Current thread:

- **ARA-2020-005: Insecure Direct Object Reference in 1CRM (CVE-2020-15958)** *Andreas Sperber (Sep 15)*

Site Search

Nmap Security Scanner
Ref Guide
Install Guide
Docs
Download
Nmap OEM

Npcap packet capture
User's Guide
API docs
Download
Npcap OEM

Security Lists
Nmap Announce
Nmap Dev
Full Disclosure
Open Source Security
BreachExchange

Security Tools
Vuln scanners
Password audit
Web scanners
Wireless
Exploitation

About
About/Contact
Privacy
Advertising
Nmap Public Source License
```