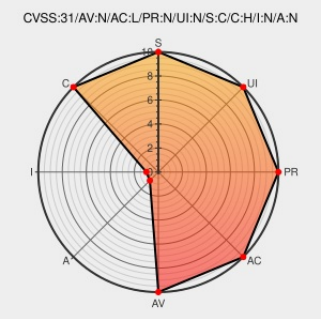
CVE-2020-15958

Published on: 09/18/2020 12:00:00 AM UTC

Last Modified on: 07/21/2021 11:39:00 AM UTC

CVE-2020-15958

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of 1crm from 1crm contain the following vulnerability:

An issue was discovered in 1CRM System through 8.6.7. An insecure direct object reference to internally stored files allows a remote attacker to access various sensitive information via an unauthenticated request with a predictable URL.

CVE-2020-15958 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.6 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	HIGH	NONE	NONE

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
Documentation « 1CRM Corp. – Customer Relationship & Business Management	Product, 1crm.com, text/html	MISC 1crm.com/documentation/
Full Disclosure: ARA-2020-005: Insecure Direct	Exploit	MISC seclists.org/fulldisclosure/2020/Sep/31

Object Reference in 1CRM (CVE-2020-15958)	Mailing List Third Party Advisory seclists.org text/html	
Sicherheitswarnung: 1CRM schützt Daten unzureichend (CVE-2020-15958) ·???? aramido	Third Party Advisory aramido.de text/html	MISC aramido.de/blog/sicherheitshinweise/sicherheitswarnung-1crm-schutzt-daten-unzureichend-cve-2020-15958
1CRM 8.6.7 Insecure Direct Object Reference ≈ Packet Storm	Exploit Third Party Advisory VDB Entry packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/159193/1CRM-8.6.7-Insecure-Direct-Object-Reference.html

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	1crm	1crm	All	All	All	All

cpe:2.3:a:1crm:1crm:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→