NEWS

X41 D-SEC GmbH Security Advisory: X41-2020-005

Unhashed Passwords Vulnerability in Smarty

Severity Rating:
High

Confirmed Affected Versions:
9.1.0

Confirmed Patched Versions:
9.1.0

Vendor:
New Media Company GmbH & Co. KG

Vendor URL:
https://www.smarty-online.de/

Vendor Reference:
-

Vector:
Local Access

Credit:
X41 D-SEC GmbH, Eric Sesterhenn

Status:
Public

CVE:
CVE-2020-10375

CWE
257

CVSS Score:
8.8

CVSS Vector:
CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

Advisory-URL:
https://www.x41-dsec.de/lab/advisories/x41-2020-005-smarty/

Summary and Impact

Passwords are stored in the database in an obfuscated format, which can be easily reverted.

Product Description

Smarty allows you to manage a medical office and patients.

Analysis

The file data.mdb contains the obfuscated passwords of users which are easily recoverable.

Proof of Concept

The second column is the obfuscated password, eg "aabbccddeeff" and "AABBCCDDEEFF".

```
$ mdb-export data.mdb  Passwd

"Heribert Topp-Glücklich","778899:::;<<",1,,1,0,1,"Topp-Glücklich","Heribert"
"Marlies Mustermann","WWXXYYZZ[[\\",0,,2,0,1,"Mustermann","Marlies"
```

Timeline

2020-02-24
Issue found

2020-03-03
Asked vendor for security contact

2020-03-04
Vendor response, technical details sent

2020-03-09
Internal fix available

2020-03-10
CVE ID CVE-2020-10375 assigned

2020-03-25
Fixed version and advisory release

About X41 D-SEC GmbH

X41 is an expert provider for application security services. Having extensive industry experience and expertise in the area of information security, a strong core security team of world class security experts enables X41 to perform premium security services.

Fields of expertise in the area of application security are security centered code reviews, binary reverse engineering and vulnerability discovery. Custom research and a IT security consulting and support services are core competencies of X41.

Author: Eric Sesterhenn
Date: March 25, 2020

«
Security in Uncertain Times - How we Handle the COVID-19 Situation at X41
»
Advisory X41-2020-003: Multiple Vulnerabilities in Epikur

CONTACT

X41 D-SEC GmbH
Krefelder Str. 123
52070 Aachen

+49 (0) 241 9809418-0
+49 (0) 241 9809418-9
info@x41-dsec.de

PGP Key