NEWS

X41 D-Sec GmbH Security Advisory: X41-2020-003

Multiple Vulnerabilities in Epikur

Highest Severity Rating:
Critical

Confirmed Affected Versions:
20.1.0.1

Confirmed Patched Versions:
20.1.1

Vendor:
Epikur Software & IT Services GmbH

Vendor URL:
https://www.epikur.de/

Credit:
X41 D-Sec GmbH, Eric Sesterhenn

Status:
Public

Advisory-URL:
https://www.x41-dsec.de/lab/advisories/x41-2020-003-epikur

Summary and Impact
Several flaws regarding authentication have been identified in Epikur, which allow attackers to access sensitive information. Among the issues identified is a backdoor password, weak password hashes and hardcoded credentials.

Product Description
Epikur allows you to manage a medical office and patients.

Backdoor Password

Severity Rating:
Critical

Vector:
Network

CVE:
CVE-2020-10539

CWE:
798

CVSS Score:
10.0

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

Analysis
The Epikur server contains the `checkPassword()` function that, upon user login, checks the submitted password against the user password's MD5 hash stored in the database. It is also compared to a second MD5 hash, which is the same for every user. If the submitted password matches either one, access is granted.

```
public boolean checkPassword(String otherPassword) {
  return (otherPassword.equals(this.passwd) || otherPassword.equals("nhEVfZUMEwwvr8b9SEpLhA=="));
}
```

Brute-forcing the second hash reveals that the password `3plkursupport` will allow you to login as any user.

Passwords stored as MD5 Hash

Severity Rating:
Medium

Vector:
Database Access

CVE:
CVE-2020-10538

CWE:
916

CVSS Score:
6.0

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

Analysis
Epikur stores the secret passwords of the users as an MD5 hash in the database. MD5 can be brute-forced efficiently and should not be used for such purposes. Additionally, since no salt is used, rainbow tables can speed up the attack.

Glassfish Administrator Password Not Set

Severity Rating:
Medium

Vector:
Local Network Interface

CVE:
CVE-2020-10537

CWE:
258

CVSS Score:
6.8

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

Analysis
A Glassfish 4.1 server with default configuration is running on TCP port 4848. No password is required to access it with the administrator account.

Timeline

2020-02-17
Issue found

2020-02-27
Asked vendor for security contact

2020-02-27
Vendor reply after just 3 hours, will setup encrypted communication channel

2020-02-28
Information sent to vendor

2020-03-10
Vendor acknoledges issues

2020-03-13
CVE IDs assigned

2020-04-01
Updated version and advisory released

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: April 01, 2020

«
Advisory X41-2020-005: Insufficient Password Protection in Smarty
»
Advisory X41-2020-004: Multiple Vulnerabilities in Medical Office

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

PGP Key

–

CONNECT

–

FAQ

Partner

Terms of Use

Privacy

Imprint