Sense of Security	Authorisation. Jason Edelstein
	Release date. 14 December 2014

Sense of Security – Security Advisory – SOS-14-004.

SAP Work Manager, SAP CRM Service Manager and iOS Client Multiple Vulnerabilities

14 December 2014.

SAP Work Manager, SAP CRM Service Manager and iOS Client - Security Advisory - SOS-14-004

Release Date.	14-Dec-2014
Last Update.	-
Vendor Notification Date.	24-Jun-2014
Product.	SAP Work Manager SAP Work Manager iOS Client SAP CRM Service Manager
Platform.	-
Affected versions.	SAP Work Manager 6.0 SAP Work Manager iOS Client SAP CRM Service Manager 4.0
Severity Rating.	Medium
Impact.	Exposure of sensitive information Exposure of system information Manipulation of data
Attack Vector.	Remote with / without authentication
Solution Status.	Vendor patch
CVE reference.	-
SAP Security Notes	2042074 2039924 2036547

Details.

Multiple vulnerabilities were detected in the SAP Work Manager 6.0, SAP Work Manager iOS Client and SAP CRM Service Manager. The security vulnerabilities can be used to enumerate remote application users, to bypass security mitigations of the platform, to obtain sensitive mobile application data, or to manipulate the application during runtime. SAP has released a series of security notes and patches to mitigate the vulnerabilities.

The SAP Agentry mobile application stores sensitive SAP data in unencrypted SQLite database files. Also the application reveals sensitive documents and files through the iOS File Sharing feature without user permission. The shared files could be changed to compromise a user's work and orders in offline usage. They could also be stolen by an attacker using unauthorised physical access, such as stolen devices or malicious chargers.

The SAP Agentry certificate pinning implementation has no signature validation and allows attackers to perform MITM attacks during the first handshake between the mobile application and the mobile service. It is possible to deploy a mobile service public key as a trusted mobile service using phishing attacks. An attacker can prepare a rogue web page to install a compromised digital certificate to the mobile device. After this step, it is possible to place a permanent rogue service between the mobile application and the mobile service. This attack vector can be used in stolen mobile device cases to extract sensitive mobile application data.

Moreover, the application binary has not been compiled with the ARC support of XCode. This makes the application binaries susceptible to memory corruption bugs, use-after free attacks and double-free attacks. An attacker can exploit a memory corruption vulnerability or identify a memory leak vulnerability easier without this mitigation technique. Also the mobile application binary and the package reveal the development environment information, users and local paths.

Finally, the mobile application logon messages and the application binary reveal sensitive system information such as valid users for the mobile application, remote services, the development environment information, and the remote system type. These can be used to obtain unauthorised access to the mobile application or the remove services.

Solution.

The following solutions are advised by SAP.

Failed logon messages have been changed to generic messages, so valid usernames can no longer be harvested. Upgrade to the latest release version to take advantage of this correction - SAP Work Manager 6.1 and SAP CRM Service Manager 4.1.

Attachments are now saved in the Application Directory folder, so when device is synced to iTunes, attachments are no longer seen in iTunes document folder. Upgrade to the latest release of SAP Work Manager 6.1 in order to take advantage of this correction.

Both the Agentry Client and the Agentry Server must be upgraded to SMP 2.3 SP04 PL01 (or greater). This corresponds to Agentry versions 6.1.4.304 (or greater). After performing the upgrade, certificate validation and client database encryption must be enabled via the instructions below.

1. The instructions for enabling certificate validation can be found in the related SAP Note 2019982 "Instructions for configuring certificates in Agentry clients and server".

2. The instructions for enabling encryption for client local storage are the following:

- Upgrade the Agentry Server, Agentry Editor, and Agentry Clients to SMP 2.3 SP04 PL01 (or greater)
- Open the Agentry application definitions in the Agentry Editor and enable "Database encryption" on the "Application Security" tab
- Publish the updated application definitions to the Agentry Server
- Transmit from each Agentry Client to encrypt each client's local database

Enable the Agentry Client's local database encryption addresses "Run time manipulation attacks on mobile application" by ensuring that all user specific data, including the username, is safely stored in the encrypted client database.

Discovered by.

Fatih Ozavci from Sense of Security Labs.

About us.

Sense of Security is a leading provider of information security and risk management solutions. Our team has expert skills in assessment and assurance, strategy and architecture, and deployment through to ongoing management. We are Australia's premier application penetration testing firm and trusted IT security advisor to many of the country's largest organisations.

Sense of Security Pty Ltd

Level 8, 66 King St
Sydney NSW 2000
AUSTRALIA

T: +61 (0)2 9290 4444
F: +61 (0)2 9290 4455
W: http://www.senseofsecurity.com.au/consulting/SAP-security
E: info@senseofsecurity.com.au
Twitter: @ITsecurityAU

The latest version of this advisory can be found at:

http://www.senseofsecurity.com.au/advisories/SOS-14-004.pdf

Other Sense of Security advisories can be found at:

http://www.senseofsecurity.com.au/research/it-security-advisories.php