Concur Travel & Expense Mobile App for iOS Information Disclosure Vulnerability

Dell SecureWorks Security Advisory SWRX-2011-002

Advisory Information

Title: Concur Travel & Expense Mobile App for iOS Information Disclosure Vulnerability
Advisory ID: SWRX-2011-002
Advisory URL: http://www.secureworks.com/research/advisories/SWRX-2011-002/
Date published: Wednesday, September 28, 2011
CVE: CVE-2011-3425
CVSS v2 Base Score: 4.7
Date of last update: Wednesday, September 28, 2011
Vendors contacted: Concur Technologies, Inc.
Release mode: Coordinated
Discovered by: Beau Woods, Dell SecureWorks

Summary

Older versions of the Concur Travel & Expense Mobile App for iOS improperly handled sensitive information. An attacker with physical or logical access to the device or to device backups could obtain the user account, password, device ID and device serial number stored on the iOS device.

Affected Products

Concur Travel & Expense Mobile App for iOS prior to version 7.3.0.0
http://www.concur.com/en-us/features/mobile

Vendor Information, Solutions and Workarounds

Prior to version 7.3.0.0, the Concur Travel & Expense Mobile App for iOS would store account credentials in cleartext within a property list file on the device. With the release of version 7.3.0.0, Concur addressed this behavior; however, a property list file created by an earlier version of the application could still be present on the device and contain cleartext account credentials. Version 8.0.0.0 removes the property list file if it is found to be present on the device.

Users of the Concur Travel & Expense Mobile App for iOS should upgrade to the latest version to address the issue.

Details

The Concur Travel & Expense Mobile App for iOS allows travelers to access the Concur travel and expense management service from the iPhone. This application provides access to account settings, expense reports, travel information, receipts, individual expenses, and other information. From the vendor's description "Concur's mobile app makes business travel and expense reporting fast, easy and secure. Use it to save expense receipts; create, review and approve business expense reports; and access business travel itineraries."[1]

Older versions of the Concur Travel & Expense Mobile App for iOS stored the account credentials in cleartext on the device. The password was stored in cleartext in a property list file on the device.

Credentials are often reused across multiple services. Therefore, disclosure of these credentials could result in multiple account compromises. The scope of the compromise could include other third-party services, as well as corporate accounts, personal email accounts, etc.

CVSS Severity (version 2.0)

Access Vector: Local
Access Complexity: Medium
Authentication: Not required to exploit
Impact Type: Information Disclosure
Confidentiality Impact: Complete
Integrity Impact: None
Availability Impact: None
CVSS v2 Base Score: 4.7
CVSS v2 Impact Subscore: 6.9
CVSS v2 Exploitability Subscore: 3.4
CVSS v2 Vector: (AV:L/AC:M/Au:N/C:C/I:N/A:N)

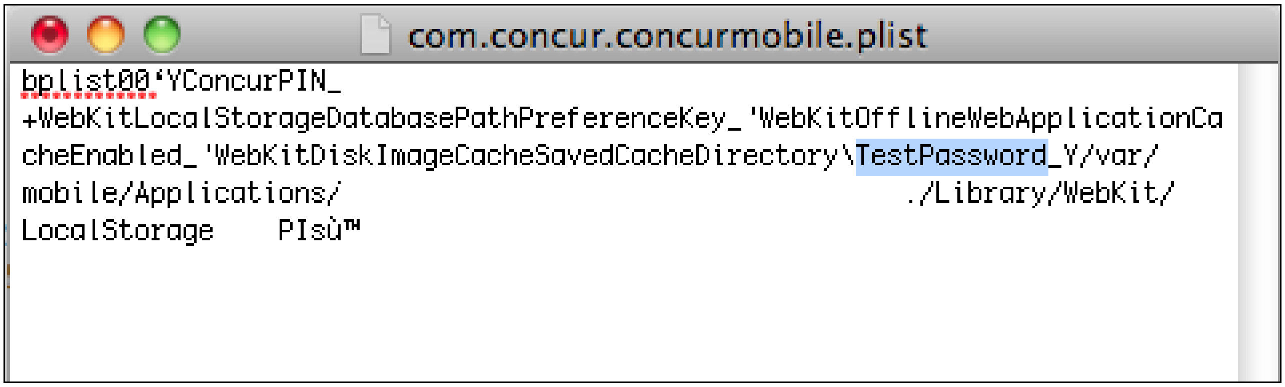
Proof of Concept

File location:
/var/mobile/Applications/**UniqueIdentifier**/Library/Preferences/com.concur.concurmobile.plist

File snippet:
[...] WebKitDiskImageCacheSavedCacheDirectory**Password**_Y/var/mobile/Applications [...]

Screenshots:

[1] http://itunes.apple.com/us/app/concur-mobile/id335023774?mt=8



```
bplist00‘YConcurPIN_
+WebKitLocalStorageDatabasePathPreferenceKey_'WebKitOfflineWebApplicationCa
cheEnabled_'WebKitDiskImageCacheSavedCacheDirectory\TestPassword_Y/var/
mobile/Applications/                                         ./Library/WebKit/
LocalStorage     PIsù™
```

Revision History

1.0 2011-09-28 – Initial advisory release

PGP Keys

This advisory has been signed with the Dell SecureWorks Counter Threat Unit℠ PGP key, which is available for download at http://www.secureworks.com/contact/SecureWorksCTU.asc.

About the Dell SecureWorks Security and Risk Consulting Team

Our Security and Risk Consulting (SRC) services help customers effectively and efficiently manage the real risks to their business. Members of our SRC team are passionate about security and have diverse security backgrounds, such as military, government, law enforcement, R&D and private industry. Our consultants are trained and experienced in audit, providing a solid understanding of control design and architecture. They are also well versed in industry standards and regulatory compliance requirements, such as PCI, GLBA, NERC CIP, HIPAA, FISMA, SOX, ISO 27001, etc. Our consultants are premier professionals and are among the most technically proficient in the industry, with broad and deep skill sets as well as a wide array of security certifications.

About Dell SecureWorks

Dell focuses exclusively on security services to protect more than 2,900 clients around the world. Dell Inc. (NASDAQ: DELL) listens to customers and delivers worldwide innovative technology and business solutions they trust and value. Recognized as an industry leader by top analysts, Dell SecureWorks provides world-class information security services to help organizations of all sizes protect their IT assets, comply with regulations and reduce security costs.

Disclaimer

The information within this advisory may change without notice. The most recent version of this advisory may be found on the Dell SecureWorks web site at www.secureworks.com for a limited period of time. Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. ANY USE OF THIS INFORMATION IS AT THE USER'S RISK. In no event shall Dell SecureWorks be liable for any damages whatsoever arising out of or in connection with the use or spread of this information.