Audible Mobile Application Information Disclosure Vulnerability

Dell SecureWorks Security Advisory SWRX-2011-004

Advisory Information

Title: Audible Mobile Application Information Disclosure Vulnerability
Advisory ID: SWRX-2011-004
Advisory URL: http://www.secureworks.com/research/advisories/SWRX-2011-004/
Date published: Friday, October 28, 2011
CVE: CVE-2011-4196
CVSS v2 Base Score: 4.7
Date of last update: Thursday, October 27, 2011
Vendors contacted: Audible, Inc.
Release mode: Coordinated
Discovered by: Beau Woods, Dell SecureWorks

Summary

The Audible for iPhone and iPod Touch (http://www.audible.com/wireless/iphone) and the Audible for Android (http://www.audible.com/wireless/android) applications improperly handle sensitive information. An attacker with physical or logical access to the device or to device backups could obtain the user account information, password, device ID and device serial number.

Affected Products

Audible for iPhone and iPod Touch versions prior to 1.7.1
Audible for Android versions prior to 1.3.5

Vendor Information, Solutions and Workarounds

Audible addressed the reported issues in version 1.7.1 of Audible for iPhone and iPod Touch and in version 1.3.5 of Audible for Android.

Details

The Audible for iPhone and iPod Touch and Audible for Android applications allow subscribers to access the service from iOS and Android-based mobile devices. These applications provide access to account settings and previously purchased selections, the ability to shop for new selections, and other functionality. From the vendor's description, "Audible.com, the Internet's premier provider of digital audiobooks and more, is now available on your iPhone and iPod Touch! This free app features the most comprehensive audiobook experience ever, including Wi-Fi delivery of your

Audible.com library, access to the Audible.com mobile store, detailed listening stats, and much more."[1]

As part of the initial authentication, the application sends an HTTP GET command to the backend server. This command includes the username, password, device ID and device serial number in the URL. The application writes a log entry for this authentication, which is stored on the device and is backed up when synced. Similar logging may occur on the Audible servers or elsewhere.

The password is either stored in cleartext or uses a trivial obfuscation scheme. The method of obfuscation is an encoding scheme where the individual characters of the cleartext password are converted to their decimal values, decremented by a constant decimal value and then converted into a hexadecimal sequence. The obfuscated hexadecimal representation of the password is prefixed by a digit that represents the decimal value used to decrement the decimal values of each character of the cleartext password. For example, the hexadecimal encoding of the string 'password' is '70617373776f7264'; using this encoding scheme, the resulting obfuscated string is '868596b6b6f676a5c' (keep in mind that the leading 8 is the decrementing prefix). The meaning of the initial prefix isn't known at publication time, but it may be the length of the username.

Example Python obfuscation and deobfuscation routines:

```
s = "password"
decrement_val = 8

def obfuscate_pass(password, neg_offset):
        obfuscated = str(neg_offset)
        for c in password:
                obfuscated += "%x" % (ord(c) - neg_offset)
        return obfuscated

def deobfuscate_pass(obfuscated):
        password = ""
        neg_offset = int(obfuscated[0])
        i = 1
        while i < len(obfuscated):
                password += chr(int(obfuscated[i] + obfuscated[i+1], 16) + neg_offset)
                i += 2
        return password

print "original string: %s" % s
print "obfuscated string: %s" % obfuscate_pass(s, decrement_val)
print "deobfuscated string: %s" % deobfuscate_pass(obfuscate_pass(s, decrement_val))
```

Credentials are often reused across multiple services. Therefore, disclosure of these credentials could result in multiple account compromises. Depending on the degree of credential reuse, the

[1] http://itunes.apple.com/us/app/audible/id379693831?mt=8

magnitude of compromise could include other third-party services, corporate accounts, personal email accounts, and more.

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

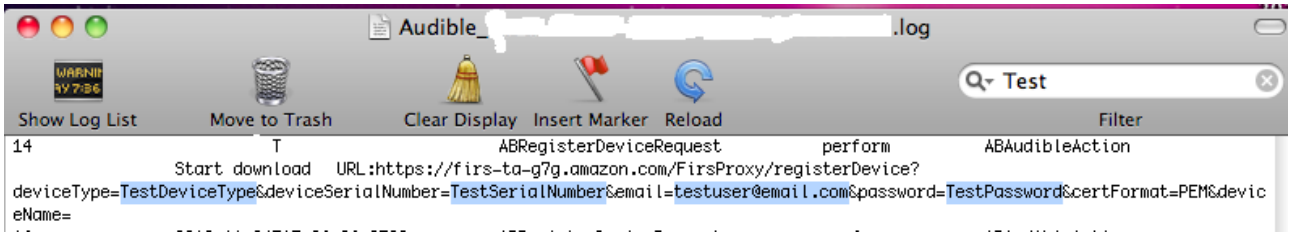
Log files can be found in:

```
/var/mobile/Applications/UniqueIdentifier/Documents/logs/Audible_Date-Time_iPhoneName_Number.log
```

A sample log entry:

```
#      Date T Time GMTOffset      ABRegisterDeviceRequest    perform      ABAudibleAction
             Start download      URL:https://firs-ta-g7g.amazon.com/FirsProxy/registerDevice?deviceType=DeviceType&deviceSerialNumber=SerialNumber&email=RegistrationEmail&password=Password&certFormat=PEM&deviceName=iPhoneName
```

Screenshot:



Revision History

1.0 2011-10-28 – 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 and ISO 27001. 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 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