Security Advisory STRAT-2012-002

Advisory Information

Advisory Title: Bambuser Mobile Application Information Disclosure Vulnerability
Internal ID: STRATSEC-2012-002
External ID: CVE Pending
Date discovered: August 10, 2012
Date reported: August 10, 2012
Date published: October 3, 2012
Current status: Vendor fix is in place
Discovered by: Beau Woods, Stratigos Security

Vendor: Bambuser (bambuser.com)
Affected product: Bambuser mobile application
Platform: iOS (confirmed); likely other versions (unconfirmed)
Vulnerable Version: 1.9.3 (confirmed); likely previous versions (unconfirmed)
Severity: 4.7 (CVSS v2)

Advisory Summary

Some versions of the Bambuser mobile application improperly handle sensitive information. An attacker with physical or logical access to the device or device backups could obtain the user account and password for the Bambuser service.

The impact to Bambuser could be reputational damage, loss of members and negative publicity.

The impact to Bambuser users could include accessing or altering the account, host unapproved streams, terminate active streams, post messages to associated social media networks and compromise of other accounts if the same account information is used across services.

Advisory Details

"Bambuser is a simple-to-use live video service that allows users to quickly and easily capture, share and watch live video through mobile phones and computers."[1]

Bambuser has a mobile application available in both the Andriod and Apple application stores, and is available for many other platforms. These applications allow Bambuser users to access their account and to watch and broadcast live video. These features require the user to login with valid account credentials.

The Bambuser mobile application does not sufficiently protect account credentials on mobile devices. The credentials are stored in plain text – that is, without encryption or hashing – in the application's file structure. Someone who gains access to the device while it is unlocked can then access this data using freely available tools. The credentials can also be obtained by gaining access to unencrypted backups which are frequently stored on the users' computers or in Apple's iCloud.

[1] http://bambuser.com/about

It may also be possible for an attacker to obtain the credentials without physical access, but through logical access – for example, through a file share, SSH or similar network services, or by using malicious software. This is especially likely if the device is rooted or jailbroken,

Potential Effects

Two primary negative consequences could affect Bambuser: reputation damage or fraud. Bambuser users may view the information leakage as a failure of Bambuser to keep their personal information protected. This could have adverse consequences in the media and press, among users and potential users and affect the Bambuser brand. This vulnerability could also potentially lead to fraudulent activity on Bambuser users' accounts – either by an attacker purchasing additional services or broadcasting streams which would consume viewing hours.

Several potential negative consequences could impact the Bambuser user. Because the attacker has the actual credentials, they can access or change account settings. For example, changing information such as the password or closing the account. The attacker could also cause reputational damage by streaming an inappropriate video or by posting to Twitter or Facebook through the Bambuser account. Or they could interrupt a broadcast, which would also cause direct financial impact. Finally, if the same account credentials are reused across sites, the attacker could gain access to other accounts and do damage there.

This issue is especially worrying when considering activists' use of Bambuser. Many of these activists must maintain the utmost concern for their privacy because their safety and sometimes their life depends on it. Given the work of anti-activist groups – primarily governments – to attempt to identify and persecute these individuals, it is likely that this vulnerability would be used by these groups for that end.

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)

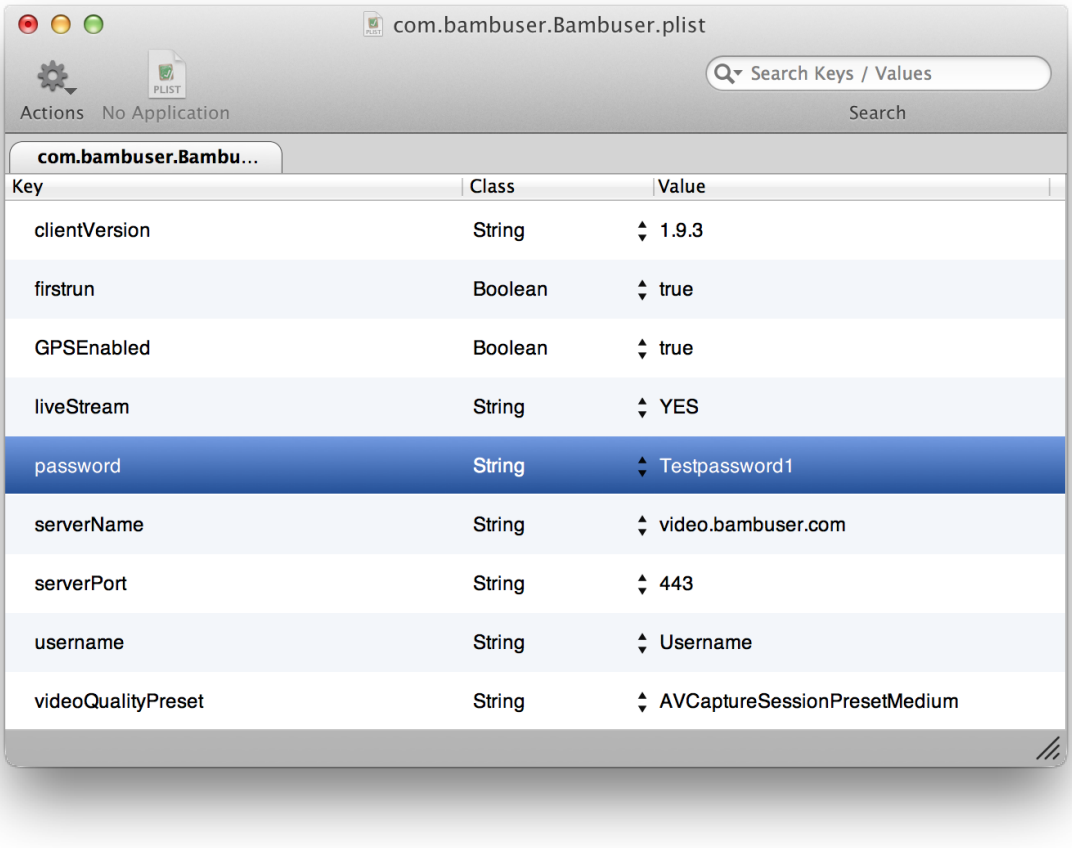
Proof of Concept

Exploit code is not required to exploit this vulnerability. The account credentials can be found in a file on the mobile device or in backup files on the computer or wherever they are stored. The path of the file on Apple iOS is:
`/var/mobile/Applications/UniqueIdentifier/Library/Preferences/com.bambuser.Bambuser.plist`

The path of the file in the iPhone backup on OS X is:
`/Users/Username/Library/Application Support/MobileSync/Backup/UniqueFilename`

Screenshot

Com.bambuser.Bambuser.plist file:



Root Cause

The root cause for this vulnerability cannot be determined with the information obtained. However, some contributory causes are likely to be related to security awareness of engineers, developers and QA staff, gaps in secure software development lifecycle (SDLC) and lack of mobile application security testing.

Recommendations

For Bambuser, Stratigos Security recommends that they immediately take action to resolve this vulnerability. This action should include not just fixing the technical problem, but putting measures in place to make internal processes more secure and publically notifying Bambuser users so they can protect themselves.

Technical fixes should ideally include the following:

- Remove the plain text account credentials from the application
- Utilize secure storage areas, such as the keychain on iOS devices

- Use tokens for authentication rather than plain text, encrypted or hashed passwords
- Ensure that Bambuser users can log out or revoke mobile app access from the web in case of loss of device.

Good internal security processes around mobile applications should ideally include the following:

- Security awareness program, including training for engineers, developers and QA staff
- Implement a secure SDLC process that begins with the requirements definition phase and continues through development, QA, implementation and maintenance. This program should focus on data security and user account security and privacy.
- Require third-parties involved in the development process to demonstrate an adequate security awareness program and secure SDLC
- Perform independent security testing of the mobile application, either by an internal group not involved in development or through a third-party.

Communication to Bambuser users should have the goal of allowing them to take measures to protect themselves and to reassure them of the security and privacy precautions Bambuser has taken.

For Bambuser users, Stratigos Security recommends that they use caution when using the Bambuser service and use good password security. Ensure that you monitor account usage and limit information that is exposed through the account. Depending on your risk tolerance, it may be advisable not to use the mobile application to prevent interference. Bambuser users should also use a strong password unique to Bambuser for the service. For any systems where you reuse account credentials, Stratigos Security **strongly** recommends changing the password to those systems as well.

About Stratigos Security

Stratigos Security is a boutique security consultancy that provides advice and guidance on information security programs, strategy and policy, as well as research and analysis. Our clients include companies large and small, from Fortune 50 to fewer than 50 employees.

Stratigos Security was founded to promote strategic and holistic approaches to security for our clients. This means taking a broad view across the organization, and in the long view, to see how and where security fits into the broader context. That is different than how many information security programs are run – compartmentalized internally and ostracized from other parts of the organization.

Stratigos Security has a published coordinated disclosure policy and process at:
http://stratigossecurity.com/about-us/coordinated-disclosure/