

# [NEWS] AudioGalaxy Username and Password Saved in Cleartext

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2001-12/0014.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 12/08/01

From: [support@securiteam.com](mailto:support@securiteam.com)

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: Sat, 8 Dec 2001 14:21:57 +0100 (CET)

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> – Know that you're safe.

-----

AudioGalaxy Username and Password Saved in Cleartext

---

## SUMMARY

<<http://www.audiogalaxy.com/>> AudioGalaxy is a website devoted to mp3's that offers an mp3 sharing program. This product stores the username and password used by the application in plain text inside a cookie – this enables everyone with access to this cookie to reveal the username and password without much effort.

## DETAILS

Sometime ago we released an

<<http://www.securiteam.com/exploits/5ZP040A3FO.html>> article about

AudioGalaxy keeping usernames and passwords in clear text in a file on the users system. Shortly after that, they fixed it, or so it seemed.

AudioGalaxy has started storing username and passwords in cookie. A sample cookie entry looks like this:

```
cookieUsername
USERNAMEHERE
audiogalaxy.com/
0
367281152
```

Securiteam: [NEWS] AudioGalaxy Username and Password Saved in Cleartext

29529638  
3457234544  
29456211

\*

cookiePassword  
CLEARTEXTPASSHERE  
audiogalaxy.com

The obvious problem is that someone exploiting the recent IE bug and stealing cookies could get the cookie and thus have the username and password. A possible scenario would be to steal the username/password, using AudioGalaxy software set an mp3 for download that the attacker has wrapped with a Trojan.

Moreover, since Back orifice does not have to have an .exe extension to infect a victim, the victim would open up an mp3 wanting to enjoy the music but rather they would be infected.

ADDITIONAL INFORMATION

The information has been provided by <mailto:[altomo@NUDEHACKERS.COM](mailto:altomo@NUDEHACKERS.COM)>  
altomo.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

[list-unsubscribe@securiteam.com](mailto:list-unsubscribe@securiteam.com)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto:list-subscribe@securiteam.com)

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

- 
- **Previous message:** [support@securiteam.com](mailto:support@securiteam.com): "[UNIX] libgtop daemon Remote Format String and Buffer Overflow Vulnerabilities"
  - **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)