

# [NT] Internet Explorer SuperCookies P3P Bypass and Cookie Controls

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-01/0076.html>

---

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

*Date:* 01/15/02

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

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

Date: Tue, 15 Jan 2002 23:15:38 +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.

-----

Internet Explorer SuperCookies P3P Bypass and Cookie Controls

---

## SUMMARY

A security hole in Internet Explorer allows the unique identification of users by requesting them to return their WMP ClientID. This ID is like a cookie, unique for each computer, allowing malicious attackers to track down the user while he roams across web sites (The vulnerability is unaffected by Microsoft's previous patch that allows disabling of "Allow Internet sites to uniquely identify your player").

## DETAILS

There is a significant privacy problem with Internet Explorer because of a design flaw in the Windows Media Player (WMP). Using a simple JavaScript code in a Web page, a Web site can grab the unique ID number of the Windows Media Player belonging to a Web site visitor. This ID number can then be used just like a cookie by the Web sites allowing him to track a user's browsing the Web.

However, this ID number becomes a SuperCookie because it can be used by Web sites to bypass all of the new privacy and P3P protections that Microsoft has added to Internet Explorer 6 (IE6). IE6 ships today with all Windows XP systems. SuperCookies also work in all previous versions

## Securiteam: [NT] Internet Explorer SuperCookies P3P Bypass and Cookie Controls

of Internet Explorer with all older versions of Windows.

Some of the other features of SuperCookies include:

- There appears to be no method of blocking SuperCookies from a Web site except to uninstall Windows Media Player or turn off JavaScript.

- All Web sites get the same ID number so they can easily exchange information about a user much like third-party cookies are used today by ad networks and Internet marketing companies.

- Even if someone is using a cookie blocker add-in, SuperCookies will still work.

- If a user has deleted cookies from his or her computer to stop tracking, a Web site can restore an old cookie value from this ID number. Once the cookie value has been restored, new tracking data can be combined with tracking data that was previously collected by the Web site.

Demonstration:

<<http://www.computerbytesman.com/privacy/supercookiedemo.htm>>  
<http://www.computerbytesman.com/privacy/supercookiedemo.htm>

This demo still works even when the WMP option "Allow Internet sites to uniquely identify your player" is turned off. This option controls when the WMP ID number is given out to Web sites when downloading streaming audio or video files, but does not appear to stop JavaScript programs from getting this number.

Technical details:

When the Windows Media Player is installed, a unique ID number in the form of a GUID is assigned to the player. This ID number is stored in the Windows registry. The ActiveX interface to the Windows Media Player allows any JavaScript Program to retrieve the ID number using the property "ClientID".

The following example HTML and JavaScript code illustrates how easy it is to retrieve the ID number:

```
<OBJECT classid="clsid:22D6F312-B0F6-11D0-94AB-0080C74C7E95" ID=WMP  
WIDTH=1 HEIGHT=1></OBJECT>
```

```
<script>  
alert(document.WMP.ClientID);  
</script>
```

Once the ID number is available to a JavaScript program, it can be sent back to a Web site by either appending it to the URL of a Web bug or storing it in regular Web browser cookie.

Recommendations for Microsoft:

One solution to this problem is for Microsoft to remove the ClientID property from the WMP ActiveX control. For compatibility with existing

## Securiteam: [NT] Internet Explorer SuperCookies P3P Bypass and Cookie Controls

JavaScript code, Microsoft may have to keep the property around, but always have it return a GUID of all zeros for all users.

An even better idea might be to remove the WMP player ID number altogether and have WMP instead use the standard cookie mechanism of Internet Explorer.

### ADDITIONAL INFORMATION

The information has been provided by <mailto:[rms@computerbytesman.com](mailto:rms@computerbytesman.com)>  
Richard M. Smith.

=====

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] Vulnerability in New User Creation in Geeklog"
  - **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)