

# [NEWS] BEA WebLogic Server Console HTML Injection

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2008-03/msg00041.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 12 Mar 2008 14:07:51 +0200
- 

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

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.  
<http://www.securiteam.com/maillinglist.html>

-----

BEA WebLogic Server Console HTML Injection

---

## SUMMARY

There is an HTML Injection vulnerability in WebLogic Server 10 Administration Console that allows the attacker to gain administrative access to the server. It is possible to craft such URL that will, when requested from the server, return a document with arbitrarily chosen HTML injected. An obvious use for this type of vulnerability is cross-site scripting that can be used, among other things, for obtaining session cookies from WebLogic administrators. These cookies, when stolen, provide the attacker with administrative access to WebLogic Administration Console, compromising the security of the entire web server.

This vulnerability is exploitable even if the Administration Console is only being accessed via HTTPS, and even if the Administrative Port is enabled.

## DETAILS

Vulnerable Systems:

- \* WebLogic Server version 10.0

## [NEWS] BEA WebLogic Server Console HTML Injection

An invalid value of some URL argument causes the Console to spawn an unhandled exception, which results in the exception stack trace being dumped onto the HTML page. The resulting exception message includes the value provided in the URL argument. While this value is partially sanitized, we found a way to bypass this sanitization and inject a working script into the resulting HTML.

In an actual attack the user would not be required to open URLs specified by the attacker. Instead, a malicious web page visited by the logged-in WebLogic administrator would mount the entire attack automatically and covertly. For instance, a tiny 0x0 pixel iframe could be used for loading the URL from the demonstration immediately upon administrator's visit to the malicious page, injecting the malicious script to the WebLogic server's response. This malicious script would then silently send these cookies to the attacker's server, where she could pick them up and use them for entering the administrator's session in the Administration Console.

### Mitigating Factors

\* In order to execute the above attack, the attacker would need to make the administrator's browser visit a malicious web page while the administrator is logged into the Administration Console. This can be achieved using social engineering, network traffic modification or a combination of both.

\* If the attacker manages to obtain a valid ADMINCONSOLESESSION cookie (and optionally \_WL\_AUTHCOOKIE\_ADMINCONSOLESESSION cookie), these will only be useful until the administrator logs out of the Administration Console. However, the attacker knowing that might rush to create a new administrative user in the console and use that user for WebLogic administration after the legitimate administrator has logged off.

### Solution:

BEA Systems has issued a <<http://dev2dev.bea.com/pub/advisory/269>> BEA08-195.00 security bulletin and published a patch which fixes this issue.

### Workaround:

\* WebLogic administrators can be trained not to browse other web pages while logged in to the Administration Console. However, since some hyperlinks in the console point to servers on the Internet (e.g., <<http://support.bea.com>> <http://support.bea.com>) the attacker could watch the administrator's Internet traffic and detect such requests as a strong sign that the administrator is currently logged in to the Administration Console. She would then slightly modify the Internet server's response so as to include the malicious code. Such an attack could only be mounted by attackers capable of monitoring and modifying the administrator's Internet traffic (most likely an ISP or someone who broke into an ISP).

\* The WebLogic Administration Console can be disabled, which would neutralize this vulnerability.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:lists@xxxxxxxx>> ACROS Security.

The original article can be found at:

<<http://www.acrossecurity.com/aspr/ASPR-2008-03-11-1-PUB.txt>>

<http://www.acrossecurity.com/aspr/ASPR-2008-03-11-1-PUB.txt>

=====

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@xxxxxxxxxxxxxxxx](mailto:list-unsubscribe@xxxxxxxxxxxxxxxx)

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

=====

=====

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.