

# [NEWS] ePortfolio Java Multiple Input Validation Vulnerabilities

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-03/msg00018.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 5 Mar 2007 19:52:12 +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>

-----

## ePortfolio Java Multiple Input Validation Vulnerabilities

---

### SUMMARY

Stefan Friedli found several web-based vulnerabilities that were identified in ePortfolio version 1.0 Java and may affect earlier versions as well.

The application uses heavy amounts of javascript code for operation. As this is not generally a bad thing, it causes massive problems when it comes to data validation. As we recognized, the entire validation of input is realized by client-side javascript which can easily be bypassed using a Proxy BURPproxy or WebScarab to modify original requests sent (and validated) by the browser.

### DETAILS

Vulnerable Systems:

\* ePortfolio version 1.0

Impact:

As there is a serious lack of server-side measured to protect the application from malicious input, an attacker may realize nearly every

[NEWS] ePortfolio Java Multiple Input Validation Vulnerabilities

attack that relies on lacking input-validation which includes Cross Site Scripting and Cross-Site Request Forgery (Session Riding).

Solution:

Server-side input validation should be provide by the application vendor as soon as possible.

Vendor Response:

The problems were recognized and will, according to the vendor, be addressed with the next release by the end of this week. Further, the vendor claims to be able to change the faulty behavior remotely or by editing a non-specified file for existing customers.

Disclosure Timeline:

- 12/22/06 – Identification of the vulnerabilities
- 02/05/07 – Notification of the vendor
- 03/02/07 – Vendor Response
- 03/02/07 – Release of public advisory

ADDITIONAL INFORMATION

The information has been provided by <<mailto:stfr@xxxxxxx>> Stefan Friedli.

The original article can be found at:

- <<http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=2893>>
- <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=2893>

=====

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

In order to subscribe to the mailing list, simply forward this email to: 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.