

Advisory 10/2006: ViewVC Undefined Charset UTF-7 XSS Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2006-10/msg00260.html>

- *From:* Stefan Esser <sesser@xxxxxxxxxxxxxxxxxxx>
 - *Date:* Sun, 15 Oct 2006 16:21:57 +0200
-

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

Happy Python Hackers Project
www.hardened-php.net

-- Security Advisory --

Advisory: ViewVC Undefined Charset UTF-7 XSS Vulnerability
Release Date: 2006/10/15
Last Modified: 2006/10/15
Author: Stefan Esser [sesser@xxxxxxxxxxxxxxxxxxx]

Application: ViewVC <= 1.0.2
Severity: A missing default charset definition allows XSS attacks against browsers interpreting UTF-7 (IE, mozilla family)
Risk: Medium
Vendor Status: Vendor released 1.0.3 which according to vendor fixes this vulnerability
References: http://www.hardened-php.net/advisory_102006.134.html

Description:

Quote from <http://www.viewvc.org>

"ViewVC is a browser interface for CVS and Subversion version control repositories. It generates templated HTML to present navigable directory, revision, and change log listings. It can display specific versions of files as well as diffs between those versions. Basically, ViewVC provides the bulk of the report-like functionality you expect out of your version control tool, but much more prettily than the average textual command-line program output."

It was discovered that ViewVC is neither sending a charset HTTP header nor specifying a charset in the HTML body. Therefore it

Advisory 10/2006: ViewVC Undefined Charset UTF-7 XSS Vulnerability

is possible to trick several browsers into decoding ViewVC pages UTF-7. This allows attackers to inject arbitrary UTF-7 encoded Java-Script code into the output.

Please note that these UTF-7 attacks against sites with missing charset definitions are also exploitable in the mozilla browser family (seamonkey, firefox, ...). Advisories from different parties that describe similar vulnerabilities usually claim that only Internet Explorer with activated auto-detection is vulnerable. In reality the mozilla browser family is even more affected, because you can attack them no matter if charset auto-detection is turned on or off.

Proof of Concept:

The Hardened-PHP Project is not going to release a proof of concept exploit to the general public.

Disclosure Timeline:

- 07. October 2006 – Notified ViewVC developers
- 13. October 2006 – ViewVC developers release 1.0.3
- 15. October 2006 – Public Disclosure

Recommendation:

It is strongly recommended to upgrade to the newest version of ViewVC 1.0.3 which you can download at:

<http://viewvc.tigris.org/servlets/ProjectDocumentList?folderID=6004>

GPG-Key:

<http://www.hardened-php.net/hardened-php-signature-key.asc>

pub 1024D/0A864AA1 2004-04-17 Hardened-PHP Signature Key
Key fingerprint = 066F A6D0 E57E 9936 9082 7E52 4439 14CC 0A86 4AA1

Copyright 2006 Stefan Esser. All rights reserved.

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.4.3 (GNU/Linux)

iD8DBQFFMICHrDkUzAqGSqERAv5fAJ0VZT36wYntwGoonHL2Q3GEEUKrCACgssem
aVuWdWmQZL1mbqnIHt81fJ8=
=cIE+

-----END PGP SIGNATURE-----