弱點掃描報告 (風險等級中以上) (Scan: tmpSCAN)

Generated on June 9, 2026 at 9:05 AM CST

Imported on June 9, 2026 at 9:05 AM CST (Scan Result ID #1753)

[C02]
NCCU

全部弱點資料

140.119.221.102

IP Address: 140.119.221.102
DNS Name: mtest.nccu.edu.tw
Score: 6
Info: 71
Low: 0
Med.: 2
High: 0
Crit.: 0
Total: 73
Vulnerabilities: Critical: 0, High: 0, Medium: 2, Low: 0, Info: 71

弱點詳細資料 - 等級Critical

Plugin	Plugin Name	Family	Protocol	Port	Exploit?

弱點詳細資料 - 等級High

Plugin	Plugin Name	Family	Protocol	Port	Exploit?

弱點詳細資料 - 等級Medium

Plugin	Plugin Name	Family	Protocol	Port	Exploit?
57640	Web Application Information Disclosure	CGI abuses	TCP	80	No

Plugin Output:

The request GET /home/search?filter=ofxfsw HTTP/1.1
Host: 140.119.221.102
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Connection: Keep-Alive
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*

produces the following path information :
</script><meta name="HandheldFriendly" content="true" /><meta name [...]
onload="tabletInit();onLoad();"
[...] iner"><form method="get" action="/home/search"><fieldset class="inputcomb [...]

The request GET /home/index?setdevice=ofxfsw HTTP/1.1
Host: 140.119.221.102
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Connection: Keep-Alive
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*

produces the following path information :
</script><meta name="HandheldFriendly" content="true" /><meta name [...]
onload="tabletInit();onLoad();onOrientationChange();"
[...] iner"><form method="get" action="/home/search"><fieldset class="inputcomb [...]

The request POST /home/index HTTP/1.1
Host: 140.119.221.102
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Content-Type: application/x-www-form-urlencoded
Connection: Keep-Alive
Cookie: 9a413b28155ba831d19c5bf733947006=r53jsm1fens691rb0o3g0tqel5; deviceClassification=%7B%22pagetype%22%3A%22compliant%22%2C%22platform%22%3A%22computer%22%2C%22browser%22%3A%22unknown%22%7D; visitID=457bbf8b4f76ab8c0effe2c8e3360f1e
Content-Length: 16
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*

setdevice=ofxfsw

produces the following path information :
</script><meta name="HandheldFriendly" content="true" /><meta name [...]
onload="tabletInit();onLoad();onOrientationChange();"
[...] iner"><form method="get" action="/home/search"><fieldset class="inputcomb [...]

Synopsis: The remote web application discloses path information.

Description: At least one web application hosted on the remote web server discloses the physical path to its directories when a malformed request is sent to it.

Leaking this kind of information may help an attacker fine-tune attacks against the application and its backend.

全部弱點資料

Steps to Remediate: Filter error messages containing path information.

See Also:

CVE:

First Discovered: May 1, 2026 09:05:13 CST

Last Observed: Jun 9, 2026 09:05:07 CST

Exploit Frameworks:

Plugin	Plugin Name	Family	Protocol	Port	Exploit?
57640	Web Application Information Disclosure	CGI abuses	TCP	443	No

Plugin Output:

The request POST /home/index HTTP/1.1
Host: 140.119.221.102
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Content-Type: application/x-www-form-urlencoded
Connection: Keep-Alive
Cookie: 9a413b28155ba831d19c5bf733947006=se58rjomkq39po43a3jli7co3k; deviceClassification=%7B%22pagetype%22%3A%22compliant%22%2C%22platform%22%3A%22computer%22%2C%22browser%22%3A%22unknown%22%7D; visitID=73a5dc519b56205587a44ee301e37b8b
Content-Length: 16
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*

setdevice=ofxfsw

produces the following path information :
</script><meta name="HandheldFriendly" content="true" /><meta name [...]
onload="tabletInit();onLoad();onOrientationChange();"
[...] iner"><form method="get" action="/home/search"><fieldset class="inputcomb [...]

The request GET /home/index?setdevice=ofxfsw HTTP/1.1
Host: 140.119.221.102
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Connection: Keep-Alive
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*

produces the following path information :
</script><meta name="HandheldFriendly" content="true" /><meta name [...]
onload="tabletInit();onLoad();onOrientationChange();"
[...] iner"><form method="get" action="/home/search"><fieldset class="inputcomb [...]

Synopsis: The remote web application discloses path information.

Description: At least one web application hosted on the remote web server discloses the physical path to its directories when a malformed request is sent to it.

Leaking this kind of information may help an attacker fine-tune attacks against the application and its backend.

Steps to Remediate: Filter error messages containing path information.

See Also:

CVE:

First Discovered: May 1, 2026 09:05:13 CST

Last Observed: Jun 9, 2026 09:05:07 CST

Exploit Frameworks:

全部弱點資料