國合處_弱點掃描報告 (Scan: Z05國合處_其他_定期掃描)

Generated on July 22, 2026 at 4:17 AM CST

Imported on July 22, 2026 at 4:17 AM CST (Scan Result ID #1849)

[maykuo]
NCCU

Table of Contents

全部弱點資料

140.119.9.77

IP Address: 140.119.9.77
DNS Name: outbound.nccu.edu.tw
Score: 4
Info: 67
Low: 1
Med.: 1
High: 0
Crit.: 0
Total: 69
Vulnerabilities: Critical: 0, High: 0, Medium: 1, Low: 1, Info: 67

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?
40984	Browsable Web Directories	CGI abuses	TCP	80	No

Plugin Output:

The following directories are browsable :

http://140.119.9.77/css/
http://140.119.9.77/css/datatables/
http://140.119.9.77/css/grapesjs/
http://140.119.9.77/css/layouts/
http://140.119.9.77/css/layouts/app/
http://140.119.9.77/css/layouts/app/dark/
http://140.119.9.77/css/layouts/app/nccu/
http://140.119.9.77/css/layouts/app/special/
http://140.119.9.77/css/layouts/app/special2/
http://140.119.9.77/css/layouts/basic/
http://140.119.9.77/images/
http://140.119.9.77/images/media/
http://140.119.9.77/images/nccu/
http://140.119.9.77/images/special/
http://140.119.9.77/images/special2/
http://140.119.9.77/js/
http://140.119.9.77/js/datatables/
http://140.119.9.77/js/grapesjs/
http://140.119.9.77/js/handlebars/
http://140.119.9.77/js/jquery-ui/
http://140.119.9.77/js/layouts/
http://140.119.9.77/js/layouts/app/
http://140.119.9.77/js/layouts/app/nccu/
http://140.119.9.77/js/layouts/app/special2/
http://140.119.9.77/js/layouts/basic/
http://140.119.9.77/js/select2/
http://140.119.9.77/storage/

Synopsis: Some directories on the remote web server are browsable.

Description: Multiple Nessus plugins identified directories on the web server that are browsable.

Steps to Remediate: Make sure that browsable directories do not leak confidential information or give access to sensitive resources. Additionally, use access restrictions or disable directory indexing for any that do.

See Also: http://www.nessus.org/u?0a35179e

CVE:

First Discovered: Jul 22, 2026 04:17:30 CST

Last Observed: Jul 22, 2026 04:17:30 CST

Exploit Frameworks:

全部弱點資料

140.119.9.53

IP Address: 140.119.9.53
DNS Name: oicchatbot.nccu.edu.tw
Score: 4
Info: 51
Low: 1
Med.: 1
High: 0
Crit.: 0
Total: 53
Vulnerabilities: Critical: 0, High: 0, Medium: 1, Low: 1, Info: 51

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?
142960	HSTS Missing From HTTPS Server (RFC 6797)	Web Servers	TCP	443	No

Plugin Output:

HTTP/1.1 200 OK

Server: nginx/1.24.0 (Ubuntu)
Date: Tue, 21 Jul 2026 20:02:46 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 20
Connection: keep-alive
X-Frame-Options: ALLOWALL
Content-Security-Policy: frame-ancestors *
X-Content-Type-Options: nosniff
Referrer-Policy: same-origin
Cross-Origin-Opener-Policy: same-origin
Vary: Origin
Content-Security-Policy:
default-src 'self';
script-src 'self' https://cdn.jsdelivr.net;
style-src 'self' https://fonts.googleapis.com;
img-src 'self' data:;
connect-src 'self' https://api.openai.com;
frame-src 'none';
frame-ancestors 'none';
font-src 'self' https://fonts.gstatic.com;
media-src 'self' data:;
object-src 'none';
manifest-src 'self';
worker-src 'self';
form-action 'self';

X-Frame-Options: DENY
X-Content-Type-Options: nosniff
Referrer-Policy: strict-origin-when-cross-origin
Permissions-Policy: geolocation=(), microphone=()

The remote HTTPS server does not send the HTTP
"Strict-Transport-Security" header.

Synopsis: The remote web server is not enforcing HSTS, as defined by RFC 6797.

Description: The remote web server is not enforcing HSTS, as defined by RFC 6797. HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

Steps to Remediate: Configure the remote web server to use HSTS.

See Also: https://tools.ietf.org/html/rfc6797

CVE:

First Discovered: Jun 19, 2025 16:44:46 CST

Last Observed: Jul 22, 2026 04:17:30 CST

Exploit Frameworks: