



CVE-2014-3428

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2014-3428
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-06-16 18:55:00 UTC
Updated	2018-10-09 19:43:00 UTC
Description	Cross-site scripting (XSS) vulnerability in Yealink VoIP Phones with firmware 28.72.0.2 allows remote attackers to inject ar

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Yealink	Voip Phone	28.2.0.128.0.0.0	All	All	All
Hardware	Yealink	Voip Phone	28.2.0.128.0.0.0	All	All	All
Operating System	Yealink	Voip Phone Firmware	28.72.0.2	All	All	All
Operating System	Yealink	Voip Phone Firmware	28.72.0.2	All	All	All

References

Reference	Source	Link
Yealink VoIP Phones XSS / CRLF Injection ≈ Packet Storm	MISC	packetstormsecu
SecurityFocus	BUGTRAQ	www.securityfocu
Full Disclosure: CVE-2014-3427 CRLF Injection and CVE-2014-3428 XSS Injection in Yealink VoIP Phones	FULLDISC	seclists.org
Yealink VoIP Phones '/servlet' Cross Site Scripting Vulnerability	BID	www.securityfocu
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)