



CVE-2006-1570

- MITRE
- NVD
- CVE.ORG
- JSON API
- Print: PDF

Summary

CVE	CVE-2006-1570
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-04-01 00:04:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Cross-site scripting (XSS) vulnerability in Esqanelapse 2.0 and 2.2 allows remote attackers to inject arbitrary web script or

Risk And Classification

Primary CVSS: v2.0 4.3 from nvd@nist.gov

AV:N/AC:M/Au:N/C:N/I:P/A:N

EPSS: 0.005270000 probability, percentile 0.671540000 (date 2026-04-17)

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

None

AV:N/AC:M/Au:N/C:N/I:P/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
------	--------	---------	---------	--------	---------	----------

Application	Esq l anelapse	Esq l anelapse	2.0	All	All	All
Application	Esq l anelapse	Esq l anelapse	2.2	All	All	All
Vendor Declared Affected Products						
Source	Vendor	Product	Version	Platforms		
CNA	Na	N/a	affected n/a	Not specified		
References						
Reference			Source	Link		
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH			af854a3a-2127-422b-91ae-364da2661108	www.vupen		
Esq l anelapse Unspecified Cross-Site Scripting Vulnerability			af854a3a-2127-422b-91ae-364da2661108	www.securi		
Esq l anelapse Unspecified Cross-Site Scripting Vulnerability - Advisories - Secunia			af854a3a-2127-422b-91ae-364da2661108	secunia.cor		
Page not found - SourceForge.net			af854a3a-2127-422b-91ae-364da2661108	sourceforge		
www.osvdb.org/24300			af854a3a-2127-422b-91ae-364da2661108	www.osvdb		
IBM X-Force Exchange			af854a3a-2127-422b-91ae-364da2661108	exchange.x		
CVE Program record			CVE.ORG	www.cve.or		
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.						