CVE-2011-3839

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

Summary

CVE	CVE-2011-3839
State	PUBLISHED
Assigner	flexera
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-12-24 19:55:03 UTC
Updated	2026-04-29 01:13:23 UTC
Description	The administration functionality in Wuzly 2.0 allows remote attackers to bypass authentication by setting the dXNlcm5hbWU

Risk And Classification

Primary CVSS: v2.0 7.5 from nvd@nist.gov

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

Problem Types: CWE-264 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wuzly	Wuzly	2.0	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source
osvdb.org/77913	af854a3a-2127-422b-91ae-364da2661
IBM X-Force Exchange	af854a3a-2127-422b-91ae-364da2661
Secunia - The Leading Provider of Vulnerability Management and Vulnerability Intelligence Solutions	af854a3a-2127-422b-91ae-364da2661
Security Advisory SA46163 - Wuzly Multiple Vulnerabilities - Secunia	af854a3a-2127-422b-91ae-364da2661
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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