# CVE-2010-2434

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

## Summary

| | |
|---|---|
| **CVE** | CVE-2010-2434 |
| **State** | PUBLISHED |
| **Assigner** | jpcert |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2010-06-25 18:30:01 UTC |
| **Updated** | 2026-04-29 01:13:23 UTC |
| **Description** | Buffer overflow in Arcext.dll 2.16.1 and earlier in pon software Explzh 5.62 and earlier allows remote attackers to execute a |

## Risk And Classification

**Primary CVSS:** v2.0 9.3 from nvd@nist.gov

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

**Problem Types:** CWE-120 | n/a

## CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

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

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Ponsoftware | Explzh | All | 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 |
|---|---|---|
| Explzsh LHA File Processing Buffer Overflow Vulnerability | af854a3a-2127-422b-91ae-364da2661108 | www.securityfo |
| 既知の不具合とその回避方法、制限事項、脆弱性情報など | af854a3a-2127-422b-91ae-364da2661108 | www.ponsoftwa |
| jvndb.jvn.jp/ja/contents/2010/JVNDB-2010-000026.html | af854a3a-2127-422b-91ae-364da2661108 | jvndb.jvn.jp |
| JVN#34729123 Explzh buffer overflow vulnerability | af854a3a-2127-422b-91ae-364da2661108 | jvn.jp |
| IBM X-Force Exchange | af854a3a-2127-422b-91ae-364da2661108 | exchange.xforc |
| Explzh LHA Processing Buffer Overflow Vulnerability - Advisories - Community | af854a3a-2127-422b-91ae-364da2661108 | secunia.com |
| osvdb.org/65666 | af854a3a-2127-422b-91ae-364da2661108 | osvdb.org |
| 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.