# CVE-2016-1142

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

## Summary

| | |
|---|---|
| **CVE** | CVE-2016-1142 |
| **State** | PUBLISHED |
| **Assigner** | jpcert |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2016-01-16 05:59:04 UTC |
| **Updated** | 2026-05-06 22:30:45 UTC |
| **Description** | Seeds acmailer before 3.8.21 and 3.9.x before 3.9.15 Beta allows remote authenticated users to execute arbitrary OS comr |

## Risk And Classification

**Primary CVSS:** v3.0 9.1 CRITICAL from nvd@nist.gov

CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H

**Problem Types:** CWE-78 | n/a

| Version | Source | Type | Score | Severity | Vector |
|---|---|---|---|---|---|
| 3.0 | nvd@nist.gov | Primary | 9.1 | CRITICAL | CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H |
| 2.0 | nvd@nist.gov | Primary | 9 | | AV:N/AC:L/Au:S/C:C/I:C/A:C |

## CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Changed

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H

## CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

Single

Confidentiality

Complete

Integrity

Complete

Availability

Complete

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

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Seeds | Acmailer | All | All | All | All |
| Application | Seeds | Acmailer | 3.9.0 | beta | All | All |
| Application | Seeds | Acmailer | 3.9.1 | beta | All | All |
| Application | Seeds | Acmailer | 3.9.10 | beta | All | All |
| Application | Seeds | Acmailer | 3.9.11 | beta | All | All |
| Application | Seeds | Acmailer | 3.9.12 | beta | All | All |
| Application | Seeds | Acmailer | 3.9.14 | All | All | All |
| Application | Seeds | Acmailer | 3.9.2 | beta | All | All |
| Application | Seeds | Acmailer | 3.9.3 | beta | All | All |
| Application | Seeds | Acmailer | 3.9.4 | beta | All | All |
| Application | Seeds | Acmailer | 3.9.5 | beta | All | All |
| Application | Seeds | Acmailer | 3.9.6 | beta | All | All |
| Application | Seeds | Acmailer | 3.9.7 | beta | All | All |
| Application | Seeds | Acmailer | 3.9.8 | beta | All | All |
| Application | Seeds | Acmailer | 3.9.9 | beta | All | All |

## Vendor Declared Affected Products

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

## References

| Reference | Source | Link |
|---|---|---|
| JVN#50899877: acmailer vulnerable to OS command injection | af854a3a-2127-422b-91ae-364da2661108 | jvn.jp |
| acmailer｜無料で使えるメール配信CGI「エーシーメーラー」｜インフォメーション | af854a3a-2127-422b-91ae-364da2661108 | www.acr |
| jvndb.jvn.jp/jvndb/JVNDB-2016-000002 | af854a3a-2127-422b-91ae-364da2661108 | jvndb.jvn |
| CVE Program record | CVE.ORG | www.cve |
| NVD vulnerability detail | NVD | nvd.nist.g |

No vendor comments have been submitted for this CVE.

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