



# CVE-2017-2175

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

|                        |                                                                                                                                |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2017-2175                                                                                                                  |
| <b>State</b>           | PUBLIC                                                                                                                         |
| <b>Assigner</b>        | vultures@jpcert.or.jp                                                                                                          |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                                   |
| <b>Published</b>       | 2017-05-22 16:29:00 UTC                                                                                                        |
| <b>Updated</b>         | 2017-05-31 13:43:00 UTC                                                                                                        |
| <b>Description</b>     | Untrusted search path vulnerability in Empirical Project Monitor - eXtended all versions allows remote attackers to gain privi |

## Risk And Classification

**Problem Types:** CWE-426

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor              | Product                                              | Version | Update | Edition | Language |
|-------------|---------------------|------------------------------------------------------|---------|--------|---------|----------|
| Application | <a href="#">Ipa</a> | <a href="#">Empirical Project Monitor - Extended</a> | -       | All    | All     | All      |
| Application | <a href="#">Ipa</a> | <a href="#">Empirical Project Monitor - Extended</a> | -       | All    | All     | All      |

## References

| Reference                                                                                                      | Source  | Link                          |
|----------------------------------------------------------------------------------------------------------------|---------|-------------------------------|
| EPM-Xにおける脆弱性の公表と提供・サポートの終了について：IPA 独立行政法人 情報処理推進機構                                                             | CONFIRM | <a href="#">www.ipa.go.jp</a> |
| JVNDB-2017-000098                                                                                              | JVNDB   | <a href="#">jvndb.jvn.jp</a>  |
| JVN#12493656: The installer of Empirical Project Monitor - eXtended may insecurely load Dynamic Link Libraries | JVN     | <a href="#">jvn.jp</a>        |
| CVE Program record                                                                                             | CVE.ORG | <a href="#">www.cve.org</a>   |
| NVD vulnerability detail                                                                                       | NVD     | <a href="#">nvd.nist.gov</a>  |

No vendor comments have been submitted for this CVE.

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

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](#).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)