



# CVE-2016-6102

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

| Summary         |                                                                                                                           |
|-----------------|---------------------------------------------------------------------------------------------------------------------------|
| CVE             | CVE-2016-6102                                                                                                             |
| State           | PUBLISHED                                                                                                                 |
| Assigner        | ibm                                                                                                                       |
| Source Priority | CVE Program / NVD first with legacy fallback                                                                              |
| Published       | 2017-03-27 22:59:00 UTC                                                                                                   |
| Updated         | 2025-04-20 01:37:25 UTC                                                                                                   |
| Description     | IBM Tivoli Key Lifecycle Manager 2.5 and 2.6 stores sensitive information in URL parameters. This may lead to information |

Risk And Classification

Primary CVSS: v3.0 3.7 LOW from nvd@nist.gov

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

Problem Types: CWE-200 | Obtain Information

| Version | Source       | Type    | Score | Severity | Vector                                       |
|---------|--------------|---------|-------|----------|----------------------------------------------|
| 3.0     | nvd@nist.gov | Primary | 3.7   | LOW      | CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N |
| 2.0     | nvd@nist.gov | Primary | 4.3   |          | AV:N/AC:M/Au:N/C:P/I:N/A:N                   |

| CVSS v3.0 Breakdown |           |
|---------------------|-----------|
| Attack Vector       | Network   |
| Attack Complexity   | High      |
| Privileges Required | None      |
| User Interaction    | None      |
| Scope               | Unchanged |
| Confidentiality     | Low       |
| Integrity           | None      |
| Availability        |           |

None

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

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor | Product                        | Version | Update | Edition | Language |
|-------------|--------|--------------------------------|---------|--------|---------|----------|
| Application | ibm    | Security Key Lifecycle Manager | 2.5.0   | All    | All     | All      |
| Application | ibm    | Security Key Lifecycle Manager | 2.5.0.0 | All    | All     | All      |
| Application | ibm    | Security Key Lifecycle Manager | 2.5.0.1 | All    | All     | All      |
| Application | ibm    | Security Key Lifecycle Manager | 2.5.0.2 | All    | All     | All      |
| Application | ibm    | Security Key Lifecycle Manager | 2.5.0.3 | All    | All     | All      |
| Application | ibm    | Security Key Lifecycle Manager | 2.5.0.4 | All    | All     | All      |
| Application | ibm    | Security Key Lifecycle Manager | 2.5.0.5 | All    | All     | All      |
| Application | ibm    | Security Key Lifecycle Manager | 2.5.0.6 | All    | All     | All      |
| Application | ibm    | Security Key Lifecycle Manager | 2.5.0.7 | All    | All     | All      |
| Application | ibm    | Security Key Lifecycle Manager | 2.6.0   | All    | All     | All      |
| Application | ibm    | Security Key Lifecycle Manager | 2.6.0.1 | All    | All     | All      |
| Application | ibm    | Security Key Lifecycle Manager | 2.6.0.2 | All    | All     | All      |

Vendor Declared Affected Products

| Source | Vendor          | Product               | Version      | Platforms     |
|--------|-----------------|-----------------------|--------------|---------------|
| CNA    | IBM Corporation | Key Lifecycle Manager | affected 2.5 | Not specified |
| CNA    | IBM Corporation | Key Lifecycle Manager | affected 2.6 | Not specified |

| References                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------------------|
| Reference                                                                                                                               |
| Security Bulletin: IBM Security Key Lifecycle Manager is affected by Query Parameter in SSL Request (CVE-2016-6102)                     |
| IBM Security Key Lifecycle Manager CVE-2016-6102 Information Disclosure Vulnerability                                                   |
| IBM Security Key Lifecycle Manager Use of URL Query Parameters Lets Remote Users Obtain Potentially Sensitive Information on the Target |
| CVE Program record                                                                                                                      |
| NVD vulnerability detail                                                                                                                |
| <div> <div></div> <div></div> </div>                                                                                                    |
| No vendor comments have been submitted for this CVE.                                                                                    |
| There are currently no legacy QID mappings associated with this CVE.                                                                    |

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)