# CVE-2021-38983

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

## Summary

| | |
|---|---|
| **CVE** | CVE-2021-38983 |
| **State** | PUBLIC |
| **Assigner** | psirt@us.ibm.com |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2021-11-15 16:15:00 UTC |
| **Updated** | 2021-11-16 19:23:00 UTC |
| **Description** | IBM Tivoli Key Lifecycle Manager 3.0, 3.0.1, 4.0, and 4.1 uses weaker than expected cryptographic algorithms that could al |

## Risk And Classification

**Problem Types:** CWE-326

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Operating System | Ibm | Aix | - | All | All | All |
| Application | Ibm | Security Guardium Key Lifecycle Manager | 4.1.0 | All | All | All |
| Application | Ibm | Security Guardium Key Lifecycle Manager | 4.1.0.1 | All | All | All |
| Application | Ibm | Security Guardium Key Lifecycle Manager | 4.1.1 | All | All | All |
| Application | Ibm | Security Key Lifecycle Manager | 4.1.0 | All | All | All |
| Application | Ibm | Security Key Lifecycle Manager | 4.1.0.1 | All | All | All |
| Application | Ibm | Security Key Lifecycle Manager | 4.1.1 | All | All | All |
| Application | Ibm | Security Key Lifecycle Manager | All | All | All | All |
| Application | Ibm | Security Key Lifecycle Manager | All | All | All | All |
| Application | Ibm | Security Key Lifecycle Manager | All | All | All | All |
| Operating System | Linux | Linux Kernel | - | All | All | All |
| Operating System | Microsoft | Windows | - | All | All | All |

## References

| Reference | Source | Link |
|---|---|---|
| Security Bulletin: Inadequate encryption strength in IBM Security Guardium Key Lifecycle Manager (CVE-2021-38983) | CONFIRM | www.ib |
| IBM X-Force Exchange | XF | exchan |

| | | |
|---|---|---|
| CVE Program record | CVE.ORG | www.cv |
| NVD vulnerability detail | NVD | nvd.nis |

No vendor comments have been submitted for this CVE.

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