



CVE-2019-3906

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

Summary

| | |
|------------------------|--|
| CVE | CVE-2019-3906 |
| State | PUBLIC |
| Assigner | vulnreport@tenable.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2019-01-18 18:29:00 UTC |
| Updated | 2022-12-03 14:45:00 UTC |
| Description | Premisys Identicard version 3.1.190 contains hardcoded credentials in the WCF service on port 9003. An authenticated ren |

Risk And Classification

Problem Types: CWE-798

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|-------------|------------|-------------|---------|--------|---------|----------|
| Application | Identicard | Premisys Id | 3.1.190 | All | All | All |
| Application | Identicard | Premisys Id | 3.1.190 | All | All | All |

References

| Reference | Source | Link | Tags |
|--|---------|--|---------------------|
| [R3] Multiple Premisys Identicard Vulnerabilities - Research Advisory Tenable® | MISC | www.tenable.com | Third Party Advisor |
| Identicard Premisys Multiple Security Vulnerabilities | BID | www.securityfocus.com | Third Party Advisor |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, analysis |

No vendor comments have been submitted for this CVE.

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

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