



# CVE-2018-6592

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

|                        |   |
|------------------------|---|
| <b>CVE</b>             | CVE-2018-6592   |
| <b>State</b>           | PUBLIC  |
| <b>Assigner</b>        | cve@mitre.org   |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback  |
| <b>Published</b>       | 2018-02-19 19:29:00 UTC   |
| <b>Updated</b>         | 2019-10-03 00:03:00 UTC   |
| <b>Description</b>     | Unisys Stealth 3.3 Windows endpoints before 3.3.016.1 allow local users to gain access to Stealth-enabled devices by leve |

## Risk And Classification

**Problem Types:** CWE-404

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor                 | Product                 | Version | Update | Edition | Language |
|-------------|------------------------|-------------------------|---------|--------|---------|----------|
| Application | <a href="#">Unisys</a> | <a href="#">Stealth</a> | All     | All    | All     | All      |
| Application | <a href="#">Unisys</a> | <a href="#">Stealth</a> | All     | All    | All     | All      |

## References

| Reference   | Source  | Link   |
|---|---------|--|
| Vulnerability Report - Memory used to store the negotiation key is not cleared or released after use. | CONFIRM | <a href="http://public.support.unisys.com">public.support.unisys.com</a> |
| CVE Program record  | CVE.ORG | <a href="http://www.cve.org">www.cve.org</a>                             |
| NVD vulnerability detail  | NVD     | <a href="http://nvd.nist.gov">nvd.nist.gov</a>                           |

No vendor comments have been submitted for this CVE.

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

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](#).

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