



# CVE-2019-5629

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

## Summary

|                        |   |
|------------------------|---|
| <b>CVE</b>             | CVE-2019-5629   |
| <b>State</b>           | PUBLIC  |
| <b>Assigner</b>        | cve@rapid7.com  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback  |
| <b>Published</b>       | 2019-07-13 01:15:00 UTC   |
| <b>Updated</b>         | 2020-10-16 15:10:00 UTC   |
| <b>Description</b>     | Rapid7 Insight Agent, version 2.6.3 and prior, suffers from a local privilege escalation due to an uncontrolled DLL search pa |

## Risk And Classification

**Problem Types:** CWE-427

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor | Product       | Version | Update | Edition | Language |
|-------------|--------|---------------|---------|--------|---------|----------|
| Application | Rapid7 | Insight Agent | All     | All    | All     | All      |

## References

| Reference  | Source   | Link   | Tags         |
|--|----------|--|--------------|
| Insight Agent Release Notes Archive - May 2019                                     | CONFIRM  | <a href="http://help.rapid7.com">help.rapid7.com</a>                 | Third Party  |
| Bugtraq: Rapid7's Windows InsightIDR Agent: Local Privilege Escalation             | BUGTRAQ  | <a href="http://seclists.org">seclists.org</a>                       | Issue Track  |
| Rapid7 Windows InsightIDR Agent 2.6.3.14 Local Privilege Escalation ~ Packet Storm | MISC     | <a href="http://packetstormsecurity.com">packetstormsecurity.com</a> | Third Party  |
| Local Privilege Escalation in Rapid7's Windows Insight IDR Agent » #bogner.sh      | MISC     | <a href="http://bogner.sh">bogner.sh</a>                             | Exploit, Thi |
| Full Disclosure: Rapid7's Windows InsightIDR Agent: Local Privilege Escalation     | FULLDISC | <a href="http://seclists.org">seclists.org</a>                       | Mailing List |
| CVE Program record   | CVE.ORG  | <a href="http://www.cve.org">www.cve.org</a>                         | canonical    |
| NVD vulnerability detail   | NVD      | <a href="http://nvd.nist.gov">nvd.nist.gov</a>                       | canonical, c |

## Vendor Comments And Credit

### Discovery Credit

**LEGACY:** This issue was discovered, and reported to Rapid7, by independent researcher Florian Bogner at Bee IT Security. It is being disclosed in accordance with Rapid7's vulnerability disclosure policy (<https://www.rapid7.com/disclosure/>).

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](#).

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