



# CVE-2020-6089

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

## Summary

|                        |                                                                                                                                  |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2020-6089                                                                                                                    |
| <b>State</b>           | PUBLIC                                                                                                                           |
| <b>Assigner</b>        | talos-cna@cisco.com                                                                                                              |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                                     |
| <b>Published</b>       | 2020-07-01 16:15:00 UTC                                                                                                          |
| <b>Updated</b>         | 2022-05-12 17:22:00 UTC                                                                                                          |
| <b>Description</b>     | An exploitable code execution vulnerability exists in the ANI file format parser of Leadtools 20. A specially crafted ANI file c |

## Risk And Classification

### Problem Types: CWE-787

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor                    | Product                   | Version    | Update | Edition | Language |
|-------------|---------------------------|---------------------------|------------|--------|---------|----------|
| Application | <a href="#">Leadtools</a> | <a href="#">Leadtools</a> | 20.0.0.0.0 | All    | All     | All      |
| Application | <a href="#">Leadtools</a> | <a href="#">Leadtools</a> | 20.0.0.0.0 | All    | All     | All      |

## References

| Reference                                                                             | Source  | Link                                                              | Tags           |
|---------------------------------------------------------------------------------------|---------|-------------------------------------------------------------------|----------------|
| TALOS-2020-1009    Cisco Talos Intelligence Group - Comprehensive Threat Intelligence | MISC    | <a href="https://talosintelligence.com">talosintelligence.com</a> | Exploit, Third |
| CVE Program record                                                                    | CVE.ORG | <a href="https://www.cve.org">www.cve.org</a>                     | canonical      |
| NVD vulnerability detail                                                              | NVD     | <a href="https://nvd.nist.gov">nvd.nist.gov</a>                   | canonical, ar  |

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](#).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)