



# CVE-2020-5734

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

## Summary

<b>CVE</b>	CVE-2020-5734
<b>State</b>	PUBLIC
<b>Assigner</b>	vulnreport@tenable.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-04-07 14:15:00 UTC
<b>Updated</b>	2020-04-07 18:40:00 UTC
<b>Description</b>	Classic buffer overflow in SolarWinds Dameware allows a remote, unauthenticated attacker to cause a denial of service by

## Risk And Classification

**Problem Types:** CWE-120

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Solarwinds</a>	<a href="#">Dameware</a>	12.1	hf3	All	All
Application	<a href="#">Solarwinds</a>	<a href="#">Dameware</a>	12.1	hf3	All	All

## References

Reference	Source	Link	Tags
SolarWinds Dameware DoS - Research Advisory   Tenable®	MISC	<a href="http://www.tenable.com">www.tenable.com</a>	Exploit, Third Party Advisory
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, analysis

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](#)**