



# CVE-2019-1350

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

## Summary

<b>CVE</b>	CVE-2019-1350
<b>State</b>	PUBLIC
<b>Assigner</b>	secure@microsoft.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-01-24 21:15:00 UTC
<b>Updated</b>	2023-11-07 03:08:00 UTC
<b>Description</b>	A remote code execution vulnerability exists when Git for Visual Studio improperly sanitizes input, aka 'Git for Visual Studio

## Risk And Classification

**Problem Types:** CWE-20

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Visual Studio 2017	All	All	All	All
Application	Microsoft	Visual Studio 2017	All	All	All	All
Application	Microsoft	Visual Studio 2019	All	All	All	All
Application	Microsoft	Visual Studio 2019	All	All	All	All

## References

Reference	Source	Link	Tags
[security-announce] openSUSE-SU-2020:0123-1: important: Security update	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>	
[security-announce] openSUSE-SU-2020:0598-1: moderate: Security update f	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>	
[ANNOUNCE] Git v2.24.1 and others - Junio C Hamano		<a href="https://public-inbox.org">public-inbox.org</a>	
Git: Multiple vulnerabilities (GLSA 202003-30) — Gentoo security	GENTOO	<a href="https://security.gentoo.org">security.gentoo.org</a>	
portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1350	MISC	<a href="https://portal.msrc.microsoft.com">portal.msrc.microsoft.com</a>	Patch, Vendor Advi
[ANNOUNCE] Git v2.24.1 and others - Junio C Hamano	MISC	<a href="https://public-inbox.org">public-inbox.org</a>	
libgit2: Multiple vulnerabilities (GLSA 202003-42) — Gentoo security	GENTOO	<a href="https://security.gentoo.org">security.gentoo.org</a>	
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, analysis

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[296076](#) Oracle Solaris 11.4 Support Repository Update (SRU) 19.3.0 Missing (CPUJAN2020)

[354769](#) Amazon Linux Security Advisory for git : ALAS2-2023-1943

[500219](#) Alpine Linux Security Update for git

[501038](#) Alpine Linux Security Update for libgit2

[501603](#) Alpine Linux Security Update for libgit2-1.0

[502112](#) Alpine Linux Security Update for libgit2-1.1

[503963](#) Alpine Linux Security Update for git

[505001](#) Alpine Linux Security Update for libgit2

© [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](#)