



# CVE-2019-6477

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

## Summary

<b>CVE</b>	CVE-2019-6477
<b>State</b>	PUBLIC
<b>Assigner</b>	security-officer@isc.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-11-26 16:15:00 UTC
<b>Updated</b>	2023-11-07 03:13:00 UTC
<b>Description</b>	With pipelining enabled each incoming query on a TCP connection requires a similar resource allocation to a query receiver

## Risk And Classification

**Problem Types:** CWE-400

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	30	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	31	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	30	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	31	All	All	All
Application	<a href="#">isc</a>	<a href="#">Bind</a>	9.11.12	s1	All	All
Application	<a href="#">isc</a>	<a href="#">Bind</a>	9.11.5	s6	All	All
Application	<a href="#">isc</a>	<a href="#">Bind</a>	9.11.6	p1	All	All
Application	<a href="#">isc</a>	<a href="#">Bind</a>	9.11.6	rc1	All	All
Application	<a href="#">isc</a>	<a href="#">Bind</a>	9.12.4	p1	All	All
Application	<a href="#">isc</a>	<a href="#">Bind</a>	9.12.4	p2	All	All
Application	<a href="#">isc</a>	<a href="#">Bind</a>	9.11.12	s1	All	All
Application	<a href="#">isc</a>	<a href="#">Bind</a>	9.11.5	s6	All	All
Application	<a href="#">isc</a>	<a href="#">Bind</a>	9.11.6	p1	All	All
Application	<a href="#">isc</a>	<a href="#">Bind</a>	9.11.6	rc1	All	All
Application	<a href="#">isc</a>	<a href="#">Bind</a>	9.12.4	p1	All	All
Application	<a href="#">isc</a>	<a href="#">Bind</a>	9.12.4	p2	All	All
Application	<a href="#">isc</a>	<a href="#">Bind</a>	All	All	All	All

Application	<a href="#">isc</a>	<a href="#">Bind</a>	All	All	All	All
Application	<a href="#">isc</a>	<a href="#">Bind</a>	All	All	All	All

## References

Reference	Source	Link
[security-announce] openSUSE-SU-2020:1699-1: moderate: Security update f	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>
[SECURITY] Fedora 30 Update: bind-dyndb-ldap-11.1-20.fc30 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
support.f5.com/csp/article/K15840535	CONFIRM	<a href="https://support.f5.com">support.f5.com</a>
[SECURITY] Fedora 30 Update: bind-dyndb-ldap-11.1-20.fc30 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
[SECURITY] Fedora 31 Update: bind-dyndb-ldap-11.2-2.fc31 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
[security-announce] openSUSE-SU-2020:1701-1: moderate: Security update f	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>
myF5		<a href="https://support.f5.com">support.f5.com</a>
Synology Inc.	CONFIRM	<a href="https://www.synology.com">www.synology.com</a>
CVE-2019-6477: TCP-pipelined queries can bypass tcp-clients limit - Security Advisories	CONFIRM	<a href="https://kb.isc.org">kb.isc.org</a>
Debian -- Security Information -- DSA-4689-1 bind9	DEBIAN	<a href="https://www.debian.org">www.debian.org</a>
[SECURITY] Fedora 31 Update: bind-dyndb-ldap-11.2-2.fc31 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[296075](#) Oracle Solaris 11.4 Support Repository Update (SRU) 21.69.0 Missing (CPUAPR2020)

[377284](#) Alibaba Cloud Linux Security Update for bind (ALINUX2-SA-2020:0083)

[500057](#) Alpine Linux Security Update for bind

[503738](#) Alpine Linux Security Update for bind

© [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](https://status.cve.report)