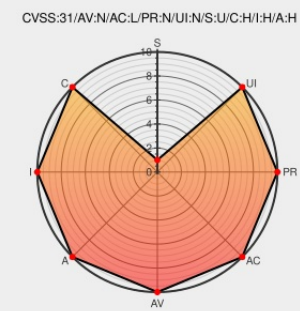
CVE-2019-19977

Published on: 12/25/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:54 PM UTC

CVE-2019-19977

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Libesmtp from Libesmtp Project contain the following vulnerability:

libESMTP through 1.0.6 mishandles domain copying into a fixed-size buffer in ntlm_build_type_2 in ntlm/ntlmstruct.c, as demonstrated by a stack-based buffer over-read.

CVE-2019-19977 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Page not found · GitHub · GitHub	Exploit Patch Third Party Advisory github.com text/html	MISC github.com/Kirin-say/Vulnerabilities/blob/master/Sta

	Inactive Link Not Archived	
libesmtp/ntlmstruct.c at ca5bd0800ef1da234315da4c59716568eb5e6402 · jbouse-debian/libesmtp · GitHub	Exploit Third Party Advisory github.com text/html	MISC github.com/jbouse-debian/libesmtp/blob/ca5bd0800ef1da234315da4c59716568e L242
libESMTP - A Library for Posting Electronic Mail	Product web.archive.org text/html	MISC web.archive.org/web/20190528215510/brianstafforc

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

751073 SUSE Enterprise Linux Security Update for libesmtp (SUSE-SU-2021:2917-1)

751089 SUSE Enterprise Linux Security Update for libesmtp (SUSE-SU-2021:2937-1)

751096 OpenSUSE Security Update for libesmtp (openSUSE-SU-2021:2937-1)

751114 OpenSUSE Security Update for libesmtp (openSUSE-SU-2021:1235-1)

901143 Common Base Linux Mariner (CBL-Mariner) Security Update for libesmtp (7260)

907027 Common Base Linux Mariner (CBL-Mariner) Security Update for libesmtp (7260-1)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Libesmtp Project	Libesmtp	All	All	All	All

cpe:2.3:a:libesmtp_project:libesmtp:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report