CVE-2026-3861

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-3861
State	PUBLISHED
Assigner	LY-Corporation
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-16 07:16:30 UTC
Updated	2026-04-17 15:38:09 UTC
Description	LINE client for iOS versions prior to 26.3.0 contains a vulnerability in the in-app browser where opening a crafted web page

Risk And Classification

Primary CVSS: v3.1 6.5 MEDIUM from dl_cve@linecorp.com

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

EPSS: 0.000130000 probability, percentile 0.021350000 (date 2026-04-21)

Problem Types: CWE-451 | na | CWE-451 CWE-451 User Interface (UI) Misrepresentation of Critical Information

Version	Source	Type	Score	Severity	Vector
3.1	dl_cve@linecorp.com	Secondary	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H
3.1	CNA	DECLARED	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

None

ntegrity

None

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	LINE Corporation	LINE Client For IOS	affected - 26.3.0 custom	Not specified

References

Reference	Source	Link	Tags
hackerone.com/reports/3422905	dl_cve@linecorp.com	hackerone.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.