Cisco Enterprise Chat and Email Lite Agent File Upload Vulnerability

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

Summary

CVE	CVE-2026-20172
State	PUBLISHED
Assigner	cisco
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-06 17:16:20 UTC
Updated	2026-05-06 18:59:53 UTC
Description	A vulnerability in the Lite Agent feature of Cisco Enterprise Chat and Email (ECE) could allow an authenticated, remote atta

Risk And Classification

Primary CVSS: v3.1 4.3 MEDIUM from psirt@cisco.com

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

Problem Types: CWE-646 | CWE-646 Reliance on File Name or Extension of Externally-Supplied File

Version	Source	Type	Score	Severity	Vector
3.1	psirt@cisco.com	Primary	4.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N
3.1	CNA	CVSSV3_1	4.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector
Network

Attack Complexity
Low

Privileges Required
Low

User Interaction
None

Scope
Unchanged

Confidentiality
None

Integrity

Low

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Cisco	Cisco Enterprise Chat And Email	affected 11.6(1)_ES3	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 11.6(1)_ES4	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.0(1)_ES6	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 11.6(1)_ES8	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.0(1)_ES5a	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 11.6(1)_ES9	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.0(1)_ES6_ET1	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 11.6(1)_ES6	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 11.6(1)_ES5	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.5(1)_ET1	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.5(1)	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.5(1)_ES3_ET1	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.0(1)_ES3	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 11.6(1)_ES11	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.0(1)_ES4	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.0(1)_ES5	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 11.6(1)_ES2	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 11.6(1)_ES9a	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 11.6(1)_ES10	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.0(1)_ES1	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.0(1)	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.5(1)_ES3	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.6(1)	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 11.5(1)	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.0(1)_ES2	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 11.6(1)_ES7	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.5(1)_ES2	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.6(1)_ET1	Not specified

CNA	Cisco	Cisco Enterprise Chat And Email	affected 11.6(1)	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.5(1)_ES1	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.6(1)_ET2	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.5(1)_ES3_ET2	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.0(1)_ES6_ET2	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.6(1)_ES1	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.5(1)_ES4	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 11.6(1)_ES12	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.6(1)_ET3	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.5(1)_ES4_ET1	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.0(1)_ES6_ET3	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.6(1)_ES1_ET1	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.6(1)_ES2	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.6_ES2_ET1	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.5(1)_ES5	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.6_ES2_ET2	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.0(1)_ES7	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.6_ES2_ET3	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.0(1)_ES7_ET1	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.5(1)_ES5_ET1	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.6_ES2_ET4	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.6(1)_ES3	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 11.6(1)_ES12_ET1	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.6_ES3_ET1	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.5(1)_ES6	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.6_ES3_ET2	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.6(1)_ES4	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.5(1)_ES7	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.6(1)_ES4_ET1	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.6(1)_ES5	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.6(1)_ES5_ET1	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.6(1)_ES5_ET2	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.6(1)_ES6	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.6(1)_ES6_ET1	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.5(1)_ES8	Not specified

CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.6(1)_ES6_ET2	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.6(1)_ES7	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.6(1)_ES8	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.6(1)_ES4_ET2	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.6(1)_ES3_ET3	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.6(1)_ES2_ET5	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.6(1)_ES1_ET2	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.6(1)_ES8_ET1	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.6(1)_ES7_ET1	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.6(1)_ES6_ET3	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.6(1)_ES5_ET3	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.5(1)_ES8_ET1	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.5(1)_ES3_ET3	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.5(1)_ES5_ET2	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.5(1)_ES6_ET1	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.5(1)_ES4_ET2	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.5(1)_ES7_ET1	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.6(1)_ES8_ET2	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.6(1)_ES9	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.6(1)_ES9_ET1	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.5(1)_ES9	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.6(1)_ES9_ET2	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.6(1)_ES9_ET3	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.6(1)_ES10	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.6(1)_ES10_ET1	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 15.0(1)	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.6(1)_ES11	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 15.0(1)_ET1	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 15.0(1)ES202508	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.6(1)_ES11_ET1	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.6(1)_ES11_ET2	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.6(1)_ES12	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 15.0(1)ES202511	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.6(1)_ES12_ET1	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 15.0(1)ES202511_ET1	Not specified
CNA	Cisco	Cisco Enterprise Chat And Email	affected 12.5(1)_ES10	Not specified

References

Reference	Source	Link	Tag
sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ece-li...	psirt@cisco.com	sec.cloudapps.cisco.com	
CVE Program record	CVE.ORG	www.cve.org	can
NVD vulnerability detail	NVD	nvd.nist.gov	can

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Exploits

CNA: The Cisco PSIRT is not aware of any public announcements or malicious use of the vulnerability that is described in this advisory.

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