



CVE-2005-2462

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

Summary

CVE	CVE-2005-2462
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-12-31 05:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Kayako liveResponse 2.x, when logging in a user, records the password in plaintext in the URL, which allows local users ar

Risk And Classification

Primary CVSS: v2.0 2.1 from nvd@nist.gov

AV:L/AC:L/Au:N/C:P/I:N/A:N

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

AV:L/AC:L/Au:N/C:P/I:N/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Kayako	Liveresponse	2.0	All	All	All

Vendor Declared Affected Products				
Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References		
Reference	Source	Link
Secunia - Advisories - Kayako LiveResponse Multiple Vulnerabilities	af854a3a-2127-422b-91ae-364da2661108	secunia.com
Contact Support	af854a3a-2127-422b-91ae-364da2661108	www.gulftech.org
www.osvdb.org/18398	af854a3a-2127-422b-91ae-364da2661108	www.osvdb.org
Kayako LiveResponse Multiple Input Validation Vulnerabilities	af854a3a-2127-422b-91ae-364da2661108	www.securityfocus.com
'Kayako liveResponse Multiple Vulnerabilities' - MARC	af854a3a-2127-422b-91ae-364da2661108	marc.info
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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