CVE-2011-1220

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

Summary

CVE	CVE-2011-1220
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-06-02 20:55:02 UTC
Updated	2026-04-29 01:13:23 UTC
Description	Stack-based buffer overflow in lcfd.exe in Tivoli Endpoint in IBM Tivoli Management Framework 3.7.1, 4.1, 4.1.1, and 4.3.1

Risk And Classification

Primary CVSS: v2.0 9 from nvd@nist.gov

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

Problem Types: CWE-119 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

Single

Confidentiality

Complete

Integrity

Complete

Availability

Complete

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ibm	Tivoli Management Framework	3.7.1	All	All	All

Application	Ibm	Tivoli Management Framework	4.1	All	All	All
Application	Ibm	Tivoli Management Framework	4.1.1	All	All	All
Application	Ibm	Tivoli Management Framework	4.3.1	All	All	All

Vendor Declared Affected Products

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

References

Reference
IBM Tivoli Management Framework lcfd Endpoint Daemon Buffer Overflow Vulnerability - Secunia.com
SecurityFocus
Zero Day Initiative
IBM Tivoli Management Framework Buffer Overflow in 'lcfd.exe' Lets Remote Authenticated Users Execute Arbitrary Code - SecurityTracker
IBM notice: The page you requested cannot be displayed
IBM Tivoli Endpoint lcfd.exe opts Argument Remote Code Execution Vulnerability - SecurityReason.com
IBM X-Force Exchange
IBM Security Vulnerability - CVE-2011-1220: IBM Tivoli Endpoint lcfd.exe opts Argument Remote Code Execution / CVE-2011-2330: IBM Tivo
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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