



CVE-2010-5109

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

Summary

CVE	CVE-2010-5109
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-05-05 17:06:02 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Off-by-one error in the DecompressRTF function in ytnef.c in Yerase's TNEF Stream Reader allows remote attackers to ca

Risk And Classification

Primary CVSS: v2.0 4.3 from nvd@nist.gov

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

Problem Types: CWE-189 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

None

Integrity

None

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	16	All	All	All

Operating System	Fedoraproject	Fedora	17	All	All	All
Application	Randall Hand	Yerases Tnef Stream Reader	-	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		
libytnef TNEF File Buffer Overflow Vulnerability			af854a3a-2127-422b-91ae-364da2661108	www.securityfocus.com		
[SECURITY] Fedora 17 Update: libytnef-1.5-8.fc17			af854a3a-2127-422b-91ae-364da2661108	lists.fedoraproject.org		
[SECURITY] Fedora 16 Update: libytnef-1.5-8.fc16			af854a3a-2127-422b-91ae-364da2661108	lists.fedoraproject.org		
831322 – (CVE-2010-5109) [PATCH] fix possible buffer overflow			af854a3a-2127-422b-91ae-364da2661108	bugzilla.redhat.com		
oss-security - CVE-2010-5109 libytnef buffer overflow			af854a3a-2127-422b-91ae-364da2661108	www.openwall.com		
Yerase's TNEF Stream Reader / Bugs / #13 Buffer Overflow in libytnef			af854a3a-2127-422b-91ae-364da2661108	sourceforge.net		
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.						