



CVE-2004-0655

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

Summary

CVE	CVE-2004-0655
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2004-08-06 04:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	eupdatedb in esearch 0.6.1 and earlier allows local users to create arbitrary files via a symlink attack on the esearchdb.py.t

Risk And Classification

Primary CVSS: v2.0 7.2 from nvd@nist.gov

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

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

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Esearch	Emerge Search Tool	0.3.1	All	All	All

Application	Esearch	Emerge Search Tool	0.4	All	All	All
Application	Esearch	Emerge Search Tool	0.4.1	All	All	All
Application	Esearch	Emerge Search Tool	0.4.2	All	All	All
Application	Esearch	Emerge Search Tool	0.5	All	All	All
Application	Esearch	Emerge Search Tool	0.5.1	All	All	All
Application	Esearch	Emerge Search Tool	0.5.2	All	All	All
Application	Esearch	Emerge Search Tool	0.5.3	All	All	All
Application	Esearch	Emerge Search Tool	0.6	All	All	All
Application	Esearch	Emerge Search Tool	0.6.1	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
Esearch eupdatedb Symbolic Link Vulnerability	af854a3a-2127-422b-91ae-364da2661108	www.securityfocus.com
Gentoo Linux Documentation -- Esearch: Insecure temp file handling	af854a3a-2127-422b-91ae-364da2661108	www.gentoo.org
IBM X-Force Exchange	af854a3a-2127-422b-91ae-364da2661108	exchange.xforce.ibmcloud.com
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.