



CVE-2004-2542

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

Summary

CVE	CVE-2004-2542
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2004-12-31 05:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Multiple SQL injection vulnerabilities in Dynix (formerly known as epixtech) WebPAC allow remote attackers to execute arbitrary code via crafted HTTP requests.

Risk And Classification

Primary CVSS: v2.0 7.5 from nvd@nist.gov

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

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

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Dynix	Webpac	All	All	All	All

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

References	
Reference	Source
SecurityTracker.com Archives - Dynix WebPAC Input Validation Holes Let Remote Users Inject SQL Commands	af854a3a-2127-422b-91ae
www.osvdb.org/9274	af854a3a-2127-422b-91ae
IBM X-Force Exchange	af854a3a-2127-422b-91ae
Dynix WebPac Multiple Undisclosed SQL Injection Vulnerabilities	af854a3a-2127-422b-91ae
Neohapsis Archives - Bugtraq - #0354 - Dynix Webpac Input Validation	af854a3a-2127-422b-91ae
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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