CVE-2005-1562

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

Summary

CVE	CVE-2005-1562
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-05-11 04:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Multiple SQL injection vulnerabilities in MaxWebPortal 1.3.5 and earlier allow remote attackers to execute arbitrary SQL cor

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	Maxwebportal	Maxwebportal	1.3.0	All	All	All

Application	Maxwebportal	Maxwebportal	1.3.1	All	All	All
Application	Maxwebportal	Maxwebportal	1.3.2	All	All	All
Application	Maxwebportal	Maxwebportal	1.3.3	All	All	All
Application	Maxwebportal	Maxwebportal	1.3.5	All	All	All
Application	Maxwebportal	Maxwebportal	1.30	All	All	All
Application	Maxwebportal	Maxwebportal	1.31	All	All	All
Application	Maxwebportal	Maxwebportal	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
www.osvdb.org/16504
'[HSC Security Group] MaxWebPortal - Multiple SQL injection/XSS' - MARC
www.osvdb.org/16510
www.osvdb.org/16506
Secunia - Advisories - MaxWebPortal Cross-Site Scripting and SQL Injection
www.osvdb.org/16502
MaxWebPortal Multiple Remote Vulnerabilities
www.osvdb.org/16503
IBM X-Force Exchange
[HSC] MaxWebPortal Multiple SQL injection and XSS : Hackers Center : Internet Security Archive: Exploits, Patch, Security Articles, Advisorie
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.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**