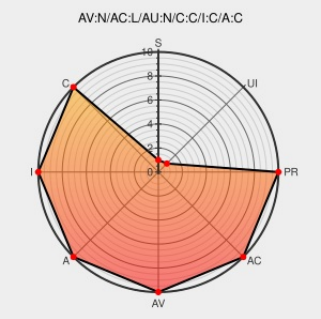
# CVE-2006-1000

Published on: 03/06/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:59 PM UTC

## CVE-2006-1000

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF




Certain versions of Pentacle In-out Board from G2soft contain the following vulnerability:

Multiple SQL injection vulnerabilities in Pentacle In-Out Board 3.0 and earlier allow remote attackers to execute arbitrary SQL commands and bypass authentication via the (1) newsid parameter to newsdetailsview.asp and (2) password parameter to login.asp.

CVE-2006-1000 has been assigned by cve@mitre.org to track the vulnerability

### CVSS2 Score: 10 - HIGH

| Access Vector | Access Complexity | Authentication |
|---|---|---|
| NETWORK | LOW | NONE |
| **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| COMPLETE | COMPLETE | COMPLETE |

### CVE References

| Description | Tags | Link |
|---|---|---|
| SecurityTracker.com Archives - Pentacle In-Out Board Input Validation Bugs in 'newsdetailsview.asp' and 'login.asp' Permit SQL Injection | Exploit, Vendor Advisory, securitytracker.com, text/html | SECTRACK 1015682 |
| SecurityFocus | www.securityfocus.com, text/html | BUGTRAQ 20060225 Advisory: Pentacle In-Out Board <= 6.03 (login.asp) AuthencationByPass Vulnerability |
| SecurityFocus | www.securityfocus.com, text/html | BUGTRAQ 20060225 Advisory: Pentacle In-Out Board <= 6.03 (newsdetailsview.aspnewsid) Remote SQL Injection Vulnerability |
| Exploit Database - Exploits for Penetration Testers, Researchers, and Ethical Hackers | Exploit, Vendor Advisory, www.nukedx.com | MISC www.nukedx.com/?viewdoc=13 |

| | | |
|---|---|---|
| | text/xml | |
| Pentacle In-Out Board Multiple SQL Injection Vulnerabilities | Exploit<br>Vendor Advisory<br>cve.report (archive)<br>text/html | BID 16818 |
| Exploit Database - Exploits for Penetration Testers, Researchers, and Ethical Hackers | Exploit<br>Vendor Advisory<br>www.nukedx.com<br>text/xml | MISC www.nukedx.com/?viewdoc=14 |
| Pentacle In-Out Board SQL Injection Vulnerabilities - Advisories - Secunia | Exploit<br>Vendor Advisory<br>web.archive.org<br>text/html | SECUNIA 19024 |
| [Full-disclosure] Advisory: Pentacle In-Out Board <= 6.03 (login.asp) Authencation ByPass Vulnerability | web.archive.org<br>text/html<br>Inactive Link Not Archived | FULLDISC 20060225 Advisory: Pentacle In-Out Board <= 6.03 (login.asp) Authencation ByPass Vulnerability |
| [Full-disclosure] Advisory: Pentacle In-Out Board <= 6.03 (newsdetailsview.asp newsid) Remote SQL Injection Vulnerability | web.archive.org<br>text/html<br>Inactive Link Not Archived | FULLDISC 20060225 Advisory: Pentacle In-Out Board <= 6.03 (newsdetailsview.asp newsid) Remote SQL Injection Vulnerability |
| Webmail : Solution de messagerie professionnelle - OVHcloud-OVH | www.vupen.com<br>text/html | VUPEN ADV-2006-0749 |

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

## Known Affected Configurations (CPE V2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | G2soft | Pentacle In-out Board | 6.03 | All | All | All |
| Application | G2soft | Pentacle In-out Board | 6.03 | All | All | All |

cpe:2.3:a:g2soft:pentacle_in-out_board:6.03:*:*:*:*:*:*:*:

cpe:2.3:a:g2soft:pentacle_in-out_board:6.03:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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