



CVE-2006-7078

Published on: 02/27/2007 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:01 PM UTC

CVE-2006-7078

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Professional Home Page Tools Login Script](#) from [Professional Home Page Tools Login Script](#) contain the following vulnerability:

Multiple cross-site scripting (XSS) vulnerabilities in Professional Home Page Tools Login Script, as of July 2006, allow remote attackers to inject arbitrary web script or HTML via the (1) name, (2) vorname, and (3) nachname parameters in the register script. NOTE: some details

have been obtained from third party sources.

CVE-2006-7078 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **4.3 - MEDIUM**

Access Vector

NETWORK

Access Complexity

MEDIUM

Authentication

NONE

Confidentiality Impact

NONE

Integrity Impact

PARTIAL

Availability Impact

NONE

CVE References

Description

Tags

Link

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

[www.vupen.com](#)
[text/html](#)

[VUPEN ADV-2006-2981](#)

[Full-disclosure] TP-Book <= 1.00 Cross Site Scripting Vulnerabilities

[web.archive.org](#)
[text/html](#)
Inactive Link **Not Archived**

[FULLDISC 20060725 Professional Home Page Tools Login Script Cross Site Scripting Vulnerabilities](#)

Professional Home Page Tools Login Script Script Insertion - Advisories - Secunia

[Vendor Advisory](#)
[web.archive.org](#)
[text/html](#)

[SECUNIA 21206](#)

CXSecurity - IDS

[securityreason.com](#)
[text/html](#)

[SREASON 2329](#)

There are currently no QIDs associated with this CVE

Type	Vendor	Product	Version	Update	Edition	Language
Application	Professional Home Page Tools Login Script	Professional Home Page Tools Login Script	All	All	All	All
Application	Professional Home Page Tools Login Script	Professional Home Page Tools Login Script	All	All	All	All

```
cpe:2.3:a:professional_home_page_tools_login_script:professional_home_page_tools_login_script:*:*:*:*:*:*:
```

Next ID→