

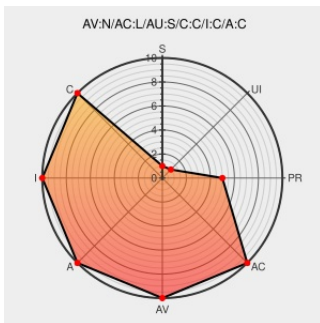


CVE-2005-4453

Published on: 12/21/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:21 PM UTC

CVE-2005-4453

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Ultraapps Issue Manager](#) from [Ultraapps](#) contain the following vulnerability:

UserProfile.cs in Ultraapps Issue Manager before 2.1 allows remote authenticated users to gain administrator privileges by modifying the original (1) p_User_user_id and (2) User_user_id parameters to UserProfile.aspx, then modifying the password field.

CVE-2005-4453 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **9 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

SINGLE

Confidentiality
Impact

COMPLETE

Integrity
Impact

COMPLETE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

Information Risk Management Plc. Tel: +44 (0)20 7808 6420

[web.archive.org](#)

[text/html](#)

Inactive Link **Not Archived**

[MISC](#)
[www.irmplc.com/advisory013.htm](#)

Webmail : Solution de messagerie professionnelle - OVHcloud-OVH

[www.vupen.com](#)

[text/html](#)

[VUPEN ADV-2005-3031](#)

SecurityFocus

[www.securityfocus.com](#)

[text/html](#)

[BUGTRAQ 20051220 IRM 013:](#)
Ultraapps Issue Manager is vulnerable to
Privilege Escalation

Ultraapps Issue Manager Privilege Escalation Vulnerability

[Patch](#)

[cve.report \(archive\)](#)

[text/html](#)

[BID 15976](#)

UltraApps Issue Manager Privilege Escalation Vulnerability -
Secunia Advisories - Vulnerability Intelligence - Secunia.com

[web.archive.org](#)

[text/html](#)

[SECUNIA 18174](#)

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	Ultraapps	Ultraapps Issue Manager	2.1	All	All	All
Application	Ultraapps	Ultraapps Issue Manager	2.1	All	All	All
cpe:2.3:a:ultraapps:ultraapps_issue_manager:2.1:*:*:*:*:*:						
cpe:2.3:a:ultraapps:ultraapps_issue_manager:2.1:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →