



CVE-2005-3650

Published on: 11/17/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:24 PM UTC

CVE-2005-3650

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

Certain versions of [First4internet Xcp Dm](#) from [First4internet Xcp Dm](#) contain the following vulnerability:

The CodeSupport.ocx ActiveX control, as used by Sony to uninstall the First4Internet XCP DRM, has "safe for scripting" enabled, which allows remote attackers to execute arbitrary code by calling vulnerable functions such as RebootMachine, IsAdministrator, and ExecuteCode.

CVE-2005-3650 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **9.3 - HIGH**

Access
Vector

NETWORK

Access
Complexity

MEDIUM

Authentication

NONE

Confidentiality
Impact

COMPLETE

Integrity
Impact

COMPLETE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

Secunia - Advisories - Sony CD First4Internet XCP Uninstallation ActiveX Control Vulnerability

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

[X SECUNIA 17610](#)

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](#)
[text/html](#)

[XF first4internet-xcp-sony-gain-access\(23063\)](#)

No Description Provided

[www.osvdb.org](#)

[OSVDB 20887](#)

Inactive Link Not Archived

Freedom to Tinker » Blog Archive » Sony's Web-Based Uninstaller Opens a Big Security Hole; Sony to Recall Discs

[www.freedom-to-tinker.com](#)
[text/html](#)

[MISC www.freedom-to-tinker.com/?p=927](#)

US-CERT Vulnerability Note VU#312073

[Third Party Advisory](#)
[US Government Resource](#)

[CERT-VN VU#312073](#)

www.kb.cert.org
text/html

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

Vendor Advisory
www.vupen.com
text/html

 VUPEN ADV-2005-2454

First 4 Internet CodeSupport Uninstallation ActiveX Software Remote Code Execution Vulnerability

[cve.report \(archive\)](#)
text/html

 BID 15430

Sony's XCP DRM

[hack.fi](#)
text/html

 MISC
hack.fi/~muzzy/sony-drm/

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	First4internet Xcp Drm	First4internet Xcp Drm	All	All	All	All
Application	First4internet Xcp Drm	First4internet Xcp Drm	All	All	All	All
cpe:2.3:a:first4internet_xcp_drm:first4internet_xcp_drm:*****:.*:						
cpe:2.3:a:first4internet_xcp_drm:first4internet_xcp_drm:*****:.*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023  |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)