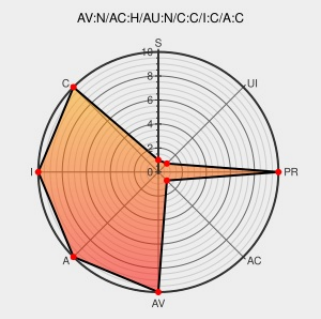
CVE-2005-3618

Published on: 12/31/2005 05:00:00 AM UTC

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

CVE-2005-3618

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



Certain versions of Esx from Vmware contain the following vulnerability:

Cross-site request forgery (CSRF) vulnerability in the management interface for VMware ESX Server 2.0.x before 2.0.2 patch 1, 2.1.x before 2.1.3 patch 1, and 2.x before 2.5.3 patch 2 allows allows remote attackers to perform unauthorized actions as the administrator via URLs, as demonstrated using the setUsr operation to change a password. NOTE: this issue can be leveraged with CVE-2005-3619 to automatically perform the attacks.

CVE-2005-3618 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.6 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	HIGH	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20060801 VMSA-2006-0004 Cross site scripting vulnerability and other fixes
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	Permissions Required Third Party Advisory www.vupen.com text/html	VUPEN ADV-2006-3075
VMware ESX Server Multiple Vulnerabilities - Advisories - Secunia	Third Party Advisory web.archive.org text/html	SECUNIA 21230

SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20060731 Corsaire Security Advisory - VMware ESX Server Password Cross Site Request Forgery issue
SecurityTracker.com Archives - VMware ESX Server URL-Based Password Change Function May Let Remote Users Change a Target User's Password in Certain Cases	Third Party Advisory VDB Entry securitytracker.com text/html	SECTRACK 1016612
VMware Knowledge Base	Vendor Advisory kb.vmware.com text/html Inactive Link Not Archived	CONFIRM kb.vmware.com/kb/2118366
	Broken Link www.corsaire.com text/plain Inactive Link Not Archived	MISC www.corsaire.com/advisories/c051114-001.txt

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
Operating System	Vmware	Esx	All	All	All	All
Operating System	Vmware	Esx	All	All	All	All

cpe:2.3:o:vmware:esx:*:*:*:*:*:*:*:*:

cpe:2.3:o:vmware:esx:*:*:*:*:*:*:*:*:

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 registred 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