

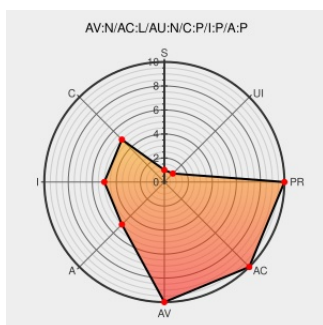


CVE-2005-1760

Published on: 06/13/2005 04:00:00 AM UTC

Last Modified on: 02/13/2023 01:09:25 AM UTC

CVE-2005-1760

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

Certain versions of [Enterprise Linux](#) from [Redhat](#) contain the following vulnerability:

sysreport 1.3.15 and earlier includes contents of the up2date file in a report, which leaks the password for a proxy server in plaintext and allows local users to gain privileges.

CVE-2005-1760 has been assigned by [secalert@redhat.com](#) to track the vulnerability

CVSS2 Score: **7.5 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

Repository / Oval Repository

[oval.cisecurity.org](#)
text/html

[OVAL](#)
[oval.org.mitre.oval:def:623](#)

Support

[Patch](#)
[Vendor Advisory](#)
[www.redhat.com](#)
text/html

[REDHAT RHSA-2005:502](#)

Sysreport May Disclose the up2date Proxy Password Via the System Report - SecurityTracker

[securitytracker.com](#)
text/html

[SECTrack 1014181](#)

RedHat Linux SysReport Proxy Information Disclosure Vulnerability

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

[BID 13936](#)

Secunia - Advisories - Red Hat update for sysreport

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

[SECUNIA 15675](#)

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	Redhat	Enterprise Linux	2.1	All	advanced_server	All
Operating System	Redhat	Enterprise Linux	2.1	All	advanced_server_ia64	All
Operating System	Redhat	Enterprise Linux	2.1	All	enterprise_server	All
Operating System	Redhat	Enterprise Linux	2.1	All	enterprise_server_ia64	All
Operating System	Redhat	Enterprise Linux	2.1	All	workstation	All
Operating System	Redhat	Enterprise Linux	2.1	All	workstation_ia64	All
Operating System	Redhat	Enterprise Linux	3.0	All	advanced_server	All
Operating System	Redhat	Enterprise Linux	3.0	All	enterprise_server	All
Operating System	Redhat	Enterprise Linux	3.0	All	workstation_server	All
Operating System	Redhat	Enterprise Linux	4.0	All	advanced_server	All
Operating System	Redhat	Enterprise Linux	4.0	All	enterprise_server	All
Operating System	Redhat	Enterprise Linux	4.0	All	workstation	All
Operating System	Redhat	Enterprise Linux	2.1	All	advanced_server	All
Operating System	Redhat	Enterprise Linux	2.1	All	advanced_server_ia64	All
Operating System	Redhat	Enterprise Linux	2.1	All	enterprise_server	All
Operating System	Redhat	Enterprise Linux	2.1	All	enterprise_server_ia64	All
Operating System	Redhat	Enterprise Linux	2.1	All	workstation	All

Operating System	Redhat	Enterprise Linux	2.1	All	workstation_ia64	All
Operating System	Redhat	Enterprise Linux	3.0	All	advanced_server	All
Operating System	Redhat	Enterprise Linux	3.0	All	enterprise_server	All
Operating System	Redhat	Enterprise Linux	3.0	All	workstation_server	All
Operating System	Redhat	Enterprise Linux	4.0	All	advanced_server	All
Operating System	Redhat	Enterprise Linux	4.0	All	enterprise_server	All
Operating System	Redhat	Enterprise Linux	4.0	All	workstation	All
Operating System	Redhat	Enterprise Linux Desktop	3.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	4.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	3.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	4.0	All	All	All
Operating System	Redhat	Linux Advanced Workstation	2.1	All	ia64	All
Operating System	Redhat	Linux Advanced Workstation	2.1	All	itanium_processor	All
Operating System	Redhat	Linux Advanced Workstation	2.1	All	ia64	All
Operating System	Redhat	Linux Advanced Workstation	2.1	All	itanium_processor	All
Application	Redhat	Sysreport	1.1	All	All	All
Application	Redhat	Sysreport	1.2	All	All	All
Application	Redhat	Sysreport	1.3	All	All	All
Application	Redhat	Sysreport	1.1	All	All	All
Application	Redhat	Sysreport	1.2	All	All	All
Application	Redhat	Sysreport	1.3	All	All	All
cpe:2.3:o:redhat:enterprise_linux:2.1*:advanced_server:****:*:						
cpe:2.3:o:redhat:enterprise_linux:2.1*:advanced_server_ia64:****:*:						
cpe:2.3:o:redhat:enterprise_linux:2.1*:enterprise_server:****:*:						
cpe:2.3:o:redhat:enterprise_linux:2.1*:enterprise_server_ia64:****:*:						
cpe:2.3:o:redhat:enterprise_linux:2.1*:workstation:****:*:						

cpe:2.3:o:redhat:enterprise_linux:2.1*:workstation_ia64:****:
cpe:2.3:o:redhat:enterprise_linux:3.0*:advanced_server:****:
cpe:2.3:o:redhat:enterprise_linux:3.0*:enterprise_server:****:
cpe:2.3:o:redhat:enterprise_linux:3.0*:workstation_server:****:
cpe:2.3:o:redhat:enterprise_linux:4.0*:advanced_server:****:
cpe:2.3:o:redhat:enterprise_linux:4.0*:enterprise_server:****:
cpe:2.3:o:redhat:enterprise_linux:4.0*:workstation:****:
cpe:2.3:o:redhat:enterprise_linux:2.1*:advanced_server:****:
cpe:2.3:o:redhat:enterprise_linux:2.1*:advanced_server_ia64:****:
cpe:2.3:o:redhat:enterprise_linux:2.1*:enterprise_server:****:
cpe:2.3:o:redhat:enterprise_linux:2.1*:enterprise_server_ia64:****:
cpe:2.3:o:redhat:enterprise_linux:2.1*:workstation:****:
cpe:2.3:o:redhat:enterprise_linux:2.1*:workstation_ia64:****:
cpe:2.3:o:redhat:enterprise_linux:3.0*:advanced_server:****:
cpe:2.3:o:redhat:enterprise_linux:3.0*:enterprise_server:****:
cpe:2.3:o:redhat:enterprise_linux:3.0*:workstation_server:****:
cpe:2.3:o:redhat:enterprise_linux:4.0*:advanced_server:****:
cpe:2.3:o:redhat:enterprise_linux:4.0*:enterprise_server:****:
cpe:2.3:o:redhat:enterprise_linux:4.0*:workstation:****:
cpe:2.3:o:redhat:enterprise_linux_desktop:3.0*:****:
cpe:2.3:o:redhat:enterprise_linux_desktop:4.0*:****:
cpe:2.3:o:redhat:enterprise_linux_desktop:3.0*:****:
cpe:2.3:o:redhat:enterprise_linux_desktop:4.0*:****:
cpe:2.3:o:redhat:linux_advanced_workstation:2.1*:ia64:****:
cpe:2.3:o:redhat:linux_advanced_workstation:2.1*:itanium_processor:****:
cpe:2.3:o:redhat:linux_advanced_workstation:2.1*:ia64:****:
cpe:2.3:o:redhat:linux_advanced_workstation:2.1*:itanium_processor:****:
cpe:2.3:a:redhat:sysreport:1.1*:****:
cpe:2.3:o:redhat:enterprise_linux:2.1*:workstation_ia64:****:

cpe:2.3:a:redhat:sysreport:1.2:*:*:*:*:*:

cpe:2.3:a:redhat:sysreport:1.3:*:*:*:*:*:

cpe:2.3:a:redhat:sysreport:1.1:*:*:*:*:*:

cpe:2.3:a:redhat:sysreport:1.2:*:*:*:*:*:

cpe:2.3:a:redhat:sysreport:1.3:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→