



CVE-1999-1115

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-1999-1115
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	1990-12-31 05:00:00 UTC
Updated	2008-09-05 20:18:00 UTC
Description	Vulnerability in the /etc/suid_exec program in HP Apollo Domain/OS sr10.2 and sr10.3 beta, related to the Korn Shell (ksh).

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Hp	Apollo Domain Os	sr10.2	All	All	All
Operating System	Hp	Apollo Domain Os	sr10.2	All	All	All
Operating System	Hp	Apollo Domain Os	All	beta	All	All

References

Reference
ISS X-Force Database: apollo-suidexec-unauthorized-access (6721): Apollo Domain/OS suid_exec program could allow unauthorized system
Domain/OS suid_exec Vulnerability
Apollo Domain/OS suid_exec Problem
CERT Advisory CA-1990-04 Apollo Domain/OS suid_exec Problem
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API [cve.report/api](#)

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