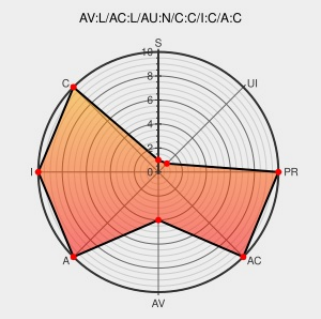
CVE-2003-1167

Published on: 12/31/2003 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:43 PM UTC

CVE-2003-1167

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



Certain versions of Kpopup from Gernot Stocker contain the following vulnerability:

misc.cpp in KPopup 0.9.1 trusts the PATH variable when executing killall, which allows local users to elevate their privileges by modifying the PATH variable to reference a malicious killall program.

CVE-2003-1167 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.2 - HIGH

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
kpopup Privileged Command Execution Vulnerability	Exploit, Patch, cve.report (archive), text/html	BID 8915
Secunia - Advisories - KPopup Privilege Escalation Vulnerability	Patch, web.archive.org, text/html	SECUNIA 10105
SecurityFocus HOME Mailing List: BugTraq	Exploit, www.securityfocus.com, text/html	BUGTRAQ 20031028 Local root vuln in kpopup
IBM X-Force Exchange	exchange.xforce.ibmcloud.com, text/html	XF kpopup-systemcall-execute-code(13540)
No Description Provided	Patch	OSVDB 2742

www.osvdb.org

Inactive Link Not Archived

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	Gernot Stocker	Kpopup	0.9.1	All	All	All
Application	Gernot Stocker	Kpopup	0.9.5_pre2	All	All	All
Application	Gernot Stocker	Kpopup	0.9.1	All	All	All
Application	Gernot Stocker	Kpopup	0.9.5_pre2	All	All	All

cpe:2.3:a:gernot_stocker:kpopup:0.9.1:*:*:*:*:*:*:*:

cpe:2.3:a:gernot_stocker:kpopup:0.9.5_pre2:*:*:*:*:*:*:*:

cpe:2.3:a:gernot_stocker:kpopup:0.9.1:*:*:*:*:*:*:*:

cpe:2.3:a:gernot_stocker:kpopup:0.9.5_pre2:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→