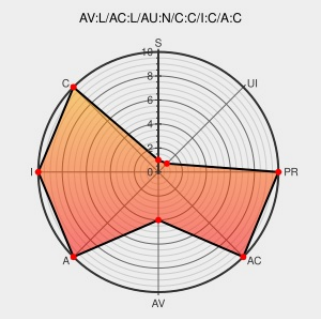
CVE-2002-2040

Published on: 12/31/2002 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:04 PM UTC

CVE-2002-2040

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



Certain versions of Rtos from Qnx contain the following vulnerability:

The (1) phrafx and (2) phgrafx-startup programs in QNX realtime operating system (RTOS) 4.25 and 6.1.0 do not properly drop privileges before executing the system command, which allows local users to execute arbitrary commands by modifying the PATH environment variable to reference a malicious crttrap program.

CVE-2002-2040 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
QNX RTOS phgrafxPrivilege Escalation Vulnerability	Exploit, cve.report (archive), text/html	BID 4915
ISS X-Force Database: qnx-rtos-phgrafx-privileges (9257): QNX RTOS phgrafx and phgrafx-startup could allow elevated privileges	web.archive.org, text/html, Inactive Link, Not Archived	XF qnx-rtos-phgrafx-privileges(9257)
SecurityFocus HOME Mailing List: BugTraq	web.archive.org, text/html, Inactive Link, Not Archived	BUGTRAQ 20020603 QNX
QNX RTOS phgrafx-startup Privilege Escalation Vulnerability	Exploit, cve.report (archive), text/html	BID 4916

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	Qnx	Rtos	4.25	All	All	All
Application	Qnx	Rtos	6.1.0	All	All	All
Application	Qnx	Rtos	4.25	All	All	All
Application	Qnx	Rtos	6.1.0	All	All	All

cpe:2.3:a:qnx:rtos:4.25:*:*:*:*:*:*:*:

cpe:2.3:a:qnx:rtos:6.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:qnx:rtos:4.25:*:*:*:*:*:*:*:

cpe:2.3:a:qnx:rtos:6.1.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→