CVE-2006-0622

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2006-0622
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-02-09 02:02:00 UTC
Updated	2017-07-20 01:29:00 UTC
Description	QNX Neutrino RTOS 6.3.0 allows local users to cause a denial of service (hang) by supplying a "break *0xb032d59f" comm

Risk And Classification

Problem Types: CWE-399

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Qnx	Rtos	6.3.0	All	All	All
Application	Qnx	Rtos	6.3.0	All	All	All

References

Reference
22960
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
SecurityTracker.com Archives - QNX RTOS Unspecified Bug Lets Local Users Deny Service and 'rc.local' Configuration Lets Local Users Gai
QNX Multiple Local Privilege Escalation and Denial Of Service Vulnerabilities
IBM X-Force Exchange
Secunia - Advisories - QNX Neutrino RTOS Multiple Privilege Escalation Vulnerabilities
Accenture | Let there be change
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 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.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**