



CVE-2008-4362

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

Summary

CVE	CVE-2008-4362
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-09-30 23:24:53 UTC
Updated	2026-04-23 00:35:47 UTC
Description	The Virtual Token driver (vdlptoken.sys) 1.0.2.43 in DESlock+ 3.2.7 allows local users to cause a denial of service (system c

Risk And Classification

Primary CVSS: v2.0 4.9 from nvd@nist.gov

AV:L/AC:L/Au:N/C:N/I:N/A:C

Problem Types: CWE-399 | n/a

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Complete

AV:L/AC:L/Au:N/C:N/I:N/A:C

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Deslock	Deslock	3.2.7	All	All	All

Vendor Declared Affected Products				
Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References	
Reference	Source
SecurityReason - DESlock+ 3.2.7 (vdlptokn.sys) Local Denial of Service Exploit	af854a3a-2127-422b-91ae-364da2661108
DESlock+ Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com	af854a3a-2127-422b-91ae-364da2661108
DESlock+ 3.2.7 - 'vdlptokn.sys' Local Denial of Service - Windows dos Exploit	af854a3a-2127-422b-91ae-364da2661108
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-91ae-364da2661108
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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