



CVE-2006-1038

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

Summary

CVE	CVE-2006-1038
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-03-07 11:02:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Buffer overflow in SecureCRT 5.0.4 and earlier and SecureFX 3.0.4 and earlier allows remote attackers to have an unknown

Risk And Classification

Primary CVSS: v2.0 10 from nvd@nist.gov

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

EPSS: 0.033310000 probability, percentile 0.873010000 (date 2026-04-16)

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
------	--------	---------	---------	--------	---------	----------

Application	Van Dyke Technologies	Securecrt	5.0	All	All	All
Application	Van Dyke Technologies	Securecrt	5.0.1	All	All	All
Application	Van Dyke Technologies	Securecrt	5.0.2	All	All	All
Application	Van Dyke Technologies	Securecrt	5.0.3	All	All	All
Application	Van Dyke Technologies	Securecrt	5.0.4	All	All	All
Application	Van Dyke Technologies	Securecrt	5.0_beta_1	All	All	All
Application	Van Dyke Technologies	Securecrt	5.0_beta_2	All	All	All
Application	Van Dyke Technologies	Securecrt	5.0_beta_3	All	All	All
Application	Van Dyke Technologies	Securecrt	5.0_beta_4	All	All	All
Application	Van Dyke Technologies	Securecrt	5.0_beta_5	All	All	All
Application	Van Dyke Technologies	Securecrt	5.0_beta_6	All	All	All
Application	Van Dyke Technologies	Securefx	3.0	All	All	All
Application	Van Dyke Technologies	Securefx	3.0.1	All	All	All
Application	Van Dyke Technologies	Securefx	3.0.2	All	All	All
Application	Van Dyke Technologies	Securefx	3.0.3	All	All	All
Application	Van Dyke Technologies	Securefx	3.0.4	All	All	All
Application	Van Dyke Technologies	Securefx	3.0_beta_1	All	All	All
Application	Van Dyke Technologies	Securefx	3.0_beta_2	All	All	All
Application	Van Dyke Technologies	Securefx	3.0_beta_3	All	All	All
Application	Van Dyke Technologies	Securefx	3.0_beta_4	All	All	All
Application	Van Dyke Technologies	Securefx	3.0_beta_5	All	All	All
Application	Van Dyke Technologies	Securefx	3.0_beta_6	All	All	All
Application	Van Dyke Technologies	Securefx	3.0_beta_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	Link
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-91ae-364da2661108	www.vup
www.vandyke.com/products/securecrt/history.txt	af854a3a-2127-422b-91ae-364da2661108	www.var
www.vandyke.com/products/securefx/history.txt	af854a3a-2127-422b-91ae-364da2661108	www.var
IBM X-Force Exchange	af854a3a-2127-422b-91ae-364da2661108	exchange
Van Dyke SecureCRT and SecureFX Buffer Overflow Vulnerability	af854a3a-2127-422b-91ae-364da2661108	www.sec
SecureCRT / SecureFX Potential Buffer Overflow Vulnerability - Advisories - Secunia	af854a3a-2127-422b-91ae-364da2661108	secunia.c

CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov
No vendor comments have been submitted for this CVE.		
There are currently no legacy QID mappings associated with this CVE.		

© [CVE.report](http://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](http://the-mitre-corporation.com) and the authoritative source of CVE content is [MITRE's CVE web site](http://mitre.org/cve). This site includes MITRE data granted under the following [license](http://mitre.org/cve).

Free CVE JSON API cve.report/api

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