# CVE-2009-2631

MITRE | NVD | CVE.ORG | Print: PDF

## Summary

| | |
|---|---|
| **CVE** | CVE-2009-2631 |
| **State** | PUBLIC |
| **Assigner** | cert@cert.org |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2009-12-04 11:30:00 UTC |
| **Updated** | 2018-10-10 19:41:00 UTC |
| **Description** | Multiple clientless SSL VPN products that run in web browsers, including Stonesoft StoneGate; Cisco ASA; SonicWALL E-( |

## Risk And Classification

**Problem Types:** CWE-264

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Hardware | Aladdin | Safenet Securewire Access Gateway | All | All | All | All |
| Hardware | Aladdin | Safenet Securewire Access Gateway | All | All | All | All |
| Hardware | Cisco | Adaptive Security Appliance | All | All | All | All |
| Hardware | Cisco | Adaptive Security Appliance | All | All | All | All |
| Hardware | Sonicwall | E-class Ssl Vpn | All | All | All | All |
| Hardware | Sonicwall | E-class Ssl Vpn | All | All | All | All |
| Hardware | Sonicwall | Ssl Vpn | All | All | All | All |
| Hardware | Sonicwall | Ssl Vpn | All | All | All | All |
| Hardware | Stonesoft | Stonegate | All | All | All | All |
| Hardware | Stonesoft | Stonegate | All | All | All | All |

## References

| Reference |
|---|
| 3 December 2009: StoneGate SSL VPN Breaks Browser Domain-Based Security – Stonesoft |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH |
| Webmail - OVH |
| www116.nortel.com/pub/repository/CLARIFY/DOCUMENT/2009/50/025367-01.pdf |

| |
|---|
| US-CERT Vulnerability Note VU#261869 |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH |
| SecurityFocus |
| Service Bulletin - SMB SRA Service Bulletin for Vulnerability CVE-2009-2631 - File INfo & Download - SonicWALL, Inc. |
| Multiple Vendor Clientless SSL VPN Products Same Origin Policy Bypass Vulnerability |
| Juniper Networks - Juniper Networks recommendations for mitigating VU#261869 - Knowledge Base |
| Full Disclosure: SSL VPNs and security |
| Nortel: Technical Support: Nortel Enterprise Response to VU#261869: Clientless SSL VPN Security Issue |
| Webmail - OVH |
| Full Disclosure: Re: SSL VPNs and security |
| IBM X-Force Exchange |
| SecurityTracker.com Archives - Cisco ASA Clientless SSL VPN Feature Lets Remote Users Bypass Web Browser Same-Origin Policy Restric |
| Full Disclosure: Re: SSL VPNs and security |
| Security Advisory SA37788 - Stonesoft StoneGate SSL VPN Same Origin Policy Bypass - Secunia |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH |
| Nortel CallPilot Web VPN Same Origin Policy Bypass - Secunia.com |
| Security Advisory SA37696 - Citrix Access Gateway Web VPN Same Origin Policy Bypass - Secunia |
| Service Bulletin - E-Class SRA Service Bulletin for Vulnerability CVE-2009-2631 - File INfo & Download - SonicWALL, Inc. |
| Juniper Networks Secure Access Web VPN Same Origin Policy Bypass - Secunia.com |
| 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.

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