



# CVE-2008-1054

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

## Summary

<b>CVE</b>	CVE-2008-1054
<b>State</b>	PUBLISHED
<b>Assigner</b>	mitre
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2008-02-27 19:44:00 UTC
<b>Updated</b>	2026-04-23 00:35:47 UTC
<b>Description</b>	Stack-based buffer overflow in the <code>_lib_spawn_user_getpid</code> function in (1) <code>swatch.exe</code> and (2) <code>surgemail.exe</code> in NetWin Sur

## Risk And Classification

**Primary CVSS:** v2.0 6.4 from nvd@nist.gov

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

**Problem Types:** CWE-119 | n/a

## CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

Partial

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

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Netwin	Surgemail	1.8a	All	All	All

Application	<a href="#">Netwin</a>	<a href="#">Surgemail</a>	1.8b3	All	All	All
Application	<a href="#">Netwin</a>	<a href="#">Surgemail</a>	1.8d	All	All	All
Application	<a href="#">Netwin</a>	<a href="#">Surgemail</a>	1.8e	All	All	All
Application	<a href="#">Netwin</a>	<a href="#">Surgemail</a>	1.8g3	All	All	All
Application	<a href="#">Netwin</a>	<a href="#">Surgemail</a>	1.9	All	All	All
Application	<a href="#">Netwin</a>	<a href="#">Surgemail</a>	1.9b2	All	All	All
Application	<a href="#">Netwin</a>	<a href="#">Surgemail</a>	2.0a2	All	All	All
Application	<a href="#">Netwin</a>	<a href="#">Surgemail</a>	2.0c	All	All	All
Application	<a href="#">Netwin</a>	<a href="#">Surgemail</a>	2.0e	All	All	All
Application	<a href="#">Netwin</a>	<a href="#">Surgemail</a>	2.0g2	All	All	All
Application	<a href="#">Netwin</a>	<a href="#">Surgemail</a>	2.1a	All	All	All
Application	<a href="#">Netwin</a>	<a href="#">Surgemail</a>	2.1c7	All	All	All
Application	<a href="#">Netwin</a>	<a href="#">Surgemail</a>	2.2a6	All	All	All
Application	<a href="#">Netwin</a>	<a href="#">Surgemail</a>	2.2c10	All	All	All
Application	<a href="#">Netwin</a>	<a href="#">Surgemail</a>	2.2c9	All	All	All
Application	<a href="#">Netwin</a>	<a href="#">Surgemail</a>	2.2g2	All	All	All
Application	<a href="#">Netwin</a>	<a href="#">Surgemail</a>	2.2g3	All	All	All
Application	<a href="#">Netwin</a>	<a href="#">Surgemail</a>	3.0a	All	All	All
Application	<a href="#">Netwin</a>	<a href="#">Surgemail</a>	3.0c2	All	All	All
Application	<a href="#">Netwin</a>	<a href="#">Surgemail</a>	3.1s	All	All	All
Application	<a href="#">Netwin</a>	<a href="#">Surgemail</a>	3.8f3	All	All	All
Application	<a href="#">Netwin</a>	<a href="#">Surgemail</a>	3.8i	All	All	All
Application	<a href="#">Netwin</a>	<a href="#">Surgemail</a>	3.8i2	All	All	All
Application	<a href="#">Netwin</a>	<a href="#">Surgemail</a>	3.8i3	All	All	All
Application	<a href="#">Netwin</a>	<a href="#">Surgemail</a>	38k	All	All	All
Application	<a href="#">Netwin</a>	<a href="#">Surgemail</a>	38k4	All	All	All

### Vendor Declared Affected Products

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

### References

Reference	Source
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-91ae-3
SecurityReason - Format string and buffer-overflow in SurgeMail 38k4	af854a3a-2127-422b-91ae-3
SurgeMail Real CGI executables Remote Buffer Overflow Vulnerability	af854a3a-2127-422b-91ae-3
SurgeMail Format String and Buffer Overflow Vulnerabilities - Advisories - Secunia	af854a3a-2127-422b-91ae-3

Surgemail Format String and Buffer Overflow vulnerabilities - Advisories - Secunia	af854a3a-2127-422b-91ae-3
alugi.altervista.org/adv/surgemailz-adv.txt	af854a3a-2127-422b-91ae-3
SecurityFocus	af854a3a-2127-422b-91ae-3
IBM X-Force Exchange	af854a3a-2127-422b-91ae-3
SurgeMail Format String and Heap Overflow May Let Remote Users Execute Arbitrary Code - SecurityTracker	af854a3a-2127-422b-91ae-3
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.

© [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](#) 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](#)