



CVE-2006-4364

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

Summary

CVE	CVE-2006-4364
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-08-27 02:04:00 UTC
Updated	2018-10-17 21:36:00 UTC
Description	Multiple heap-based buffer overflows in the POP3 server in Alt-N Technologies MDAemon before 9.0.6 allow remote attack

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Alt-n	Mdaemon	2.71_sp1	All	All	All
Application	Alt-n	Mdaemon	2.8	All	All	All
Application	Alt-n	Mdaemon	2.8.5.0	All	All	All
Application	Alt-n	Mdaemon	3.0.3	All	All	All
Application	Alt-n	Mdaemon	3.0.4	All	All	All
Application	Alt-n	Mdaemon	3.1.1	All	All	All
Application	Alt-n	Mdaemon	3.1.2	All	All	All
Application	Alt-n	Mdaemon	3.1_beta	All	All	All
Application	Alt-n	Mdaemon	3.5.0	All	All	All
Application	Alt-n	Mdaemon	3.5.1	All	All	All
Application	Alt-n	Mdaemon	3.5.4	All	All	All
Application	Alt-n	Mdaemon	3.5.4	All	pro	All
Application	Alt-n	Mdaemon	3.5.4	All	standard	All
Application	Alt-n	Mdaemon	3.5.6	All	All	All
Application	Alt-n	Mdaemon	5.0	All	All	All
Application	Alt-n	Mdaemon	5.0	All	pro	All
Application	Alt-n	Mdaemon	5.0.1	All	All	All

Application	Alt-n	Mdaemon	5.0.2	All	All	All
Application	Alt-n	Mdaemon	5.0.3	All	All	All
Application	Alt-n	Mdaemon	5.0.4	All	All	All
Application	Alt-n	Mdaemon	5.0.5	All	All	All
Application	Alt-n	Mdaemon	5.0.6	All	All	All
Application	Alt-n	Mdaemon	5.0.7	All	All	All
Application	Alt-n	Mdaemon	6.0	All	All	All
Application	Alt-n	Mdaemon	6.0.5	All	All	All
Application	Alt-n	Mdaemon	6.0.6	All	All	All
Application	Alt-n	Mdaemon	6.0.7	All	All	All
Application	Alt-n	Mdaemon	6.5.0	All	All	All
Application	Alt-n	Mdaemon	6.5.1	All	All	All
Application	Alt-n	Mdaemon	6.5.2	All	All	All
Application	Alt-n	Mdaemon	6.7.5	All	All	All
Application	Alt-n	Mdaemon	6.7.9	All	All	All
Application	Alt-n	Mdaemon	6.8.0	All	All	All
Application	Alt-n	Mdaemon	6.8.1	All	All	All
Application	Alt-n	Mdaemon	6.8.2	All	All	All
Application	Alt-n	Mdaemon	6.8.3	All	All	All
Application	Alt-n	Mdaemon	6.8.4	All	All	All
Application	Alt-n	Mdaemon	6.8.5	All	All	All
Application	Alt-n	Mdaemon	7.2	All	All	All
Application	Alt-n	Mdaemon	8.1.1	All	All	All
Application	Alt-n	Mdaemon	8.1.3	All	All	All
Application	Alt-n	Mdaemon	8.1.4	All	All	All
Application	Alt-n	Mdaemon	9.0.1	All	All	All
Application	Alt-n	Mdaemon	9.0.2	All	All	All
Application	Alt-n	Mdaemon	9.0.3	All	All	All
Application	Alt-n	Mdaemon	9.0.4	All	All	All
Application	Alt-n	Mdaemon	9.0.5	All	All	All
Application	Alt-n	Mdaemon	2.71_sp1	All	All	All
Application	Alt-n	Mdaemon	2.8	All	All	All
Application	Alt-n	Mdaemon	2.8.5.0	All	All	All
Application	Alt-n	Mdaemon	3.0.3	All	All	All
Application	Alt-n	Mdaemon	3.0.4	All	All	All

Application	Alt-n	Mdaemon	3.1.1	All	All	All
Application	Alt-n	Mdaemon	3.1.2	All	All	All
Application	Alt-n	Mdaemon	3.1_beta	All	All	All
Application	Alt-n	Mdaemon	3.5.0	All	All	All
Application	Alt-n	Mdaemon	3.5.1	All	All	All
Application	Alt-n	Mdaemon	3.5.4	All	All	All
Application	Alt-n	Mdaemon	3.5.4	All	pro	All
Application	Alt-n	Mdaemon	3.5.4	All	standard	All
Application	Alt-n	Mdaemon	3.5.6	All	All	All
Application	Alt-n	Mdaemon	5.0	All	All	All
Application	Alt-n	Mdaemon	5.0	All	pro	All
Application	Alt-n	Mdaemon	5.0.1	All	All	All
Application	Alt-n	Mdaemon	5.0.2	All	All	All
Application	Alt-n	Mdaemon	5.0.3	All	All	All
Application	Alt-n	Mdaemon	5.0.4	All	All	All
Application	Alt-n	Mdaemon	5.0.5	All	All	All
Application	Alt-n	Mdaemon	5.0.6	All	All	All
Application	Alt-n	Mdaemon	5.0.7	All	All	All
Application	Alt-n	Mdaemon	6.0	All	All	All
Application	Alt-n	Mdaemon	6.0.5	All	All	All
Application	Alt-n	Mdaemon	6.0.6	All	All	All
Application	Alt-n	Mdaemon	6.0.7	All	All	All
Application	Alt-n	Mdaemon	6.5.0	All	All	All
Application	Alt-n	Mdaemon	6.5.1	All	All	All
Application	Alt-n	Mdaemon	6.5.2	All	All	All
Application	Alt-n	Mdaemon	6.7.5	All	All	All
Application	Alt-n	Mdaemon	6.7.9	All	All	All
Application	Alt-n	Mdaemon	6.8.0	All	All	All
Application	Alt-n	Mdaemon	6.8.1	All	All	All
Application	Alt-n	Mdaemon	6.8.2	All	All	All
Application	Alt-n	Mdaemon	6.8.3	All	All	All
Application	Alt-n	Mdaemon	6.8.4	All	All	All
Application	Alt-n	Mdaemon	6.8.5	All	All	All
Application	Alt-n	Mdaemon	7.2	All	All	All
Application	Alt-n	Mdaemon	8.1.1	All	All	All

Application	Alt-n	Mdaemon	8.1.3	All	All	All
Application	Alt-n	Mdaemon	8.1.4	All	All	All
Application	Alt-n	Mdaemon	9.0.1	All	All	All
Application	Alt-n	Mdaemon	9.0.2	All	All	All
Application	Alt-n	Mdaemon	9.0.3	All	All	All
Application	Alt-n	Mdaemon	9.0.4	All	All	All
Application	Alt-n	Mdaemon	9.0.5	All	All	All

References

Reference	Source
Alt-N MDAemon Multiple Remote Pre-Authentication POP3 Buffer Overflow Vulnerabilities	BID
MDaemon Release Notes	CO
MDaemon POP3 Server Buffer Overflow Vulnerabilities - Advisories - Secunia	SE
SecurityFocus	BU
MDaemon POP3 Server < 9.06 (USER) Remote Buffer Overflow PoC	EX
INFIGO IS Security Advisory #INFIGO-2006-08-04 Infigo	MI
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VU
SecurityReason - MDAemon POP3 server remote buffer overflow (preauth)	SR
IBM X-Force Exchange	XF
28125	OS
SecurityTracker.com Archives - MDAemon Buffer Overflow in USER and APOP Commands Lets Remote Users Execute Arbitrary Code	SE
CVE Program record	CV
NVD vulnerability detail	NV

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](#)