



CVE-2008-1279

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

Summary

CVE	CVE-2008-1279
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-03-10 23:44:00 UTC
Updated	2018-10-11 20:31:00 UTC
Description	Acronis True Image Group Server 1.5.19.191 and earlier, included in Acronis True Image Enterprise Server 9.5.0.8072 and

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Acronis	True Image	All	All	group_server	All
Application	Acronis	True Image	All	All	enterprise_server	All

References

Reference

IBM X-Force Exchange
aluiigi.altervista.org/adv/acrogroup-adv.txt
SecurityFocus
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
Acronis True Image Echo Group Server and Windows Agent Denial of Service - Secunia Advisories - Vulnerability Intelligence - Secunia.com
Acronis True Image Echo Enterprise Server Multiple Remote Denial of Service Vulnerabilities
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 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](#)