



CVE-2001-0820

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

Summary

CVE	CVE-2001-0820
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2001-12-06 05:00:00 UTC
Updated	2017-12-19 02:29:00 UTC
Description	Buffer overflows in GazTek ghttpd 1.4 allows a remote attacker to execute arbitrary code via long arguments that are passe

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gaztek	Ghttp	1.4	All	All	All
Application	Gaztek	Ghttp	1.4	All	All	All

References

Reference	Source	Link
IBM X-Force Exchange	XF	excha
Sorry, the content you are trying to view does not exist. If you feel this message is in error, please email the webmaster.	BID	www.
ghttpd Daemon Buffer Overflow Vulnerability	BID	www.
'Buffer Overflow in GazTek HTTP Daemon v1.4 (ghttpd)' - MARC	BUGTRAQ	marc.
20010630 Advisory Ghttp 1.4	BUGTRAQ	marc.
CVE Program record	CVE.ORG	www.
NVD vulnerability detail	NVD	nvd.n

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](#)