



CVE-2004-2518

Published on: 12/31/2004 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:14 PM UTC

CVE-2004-2518

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Gattaca Server 2003](#) from [Geeos Team](#) contain the following vulnerability:

Gattaca Server 2003 1.1.10.0 allows remote attackers to obtain sensitive information via (1) a trailing null byte ("%00") to a URL or (2) an invalid LANGUAGE parameter to web.tmpl, which reveals the full installation path in an error message.

CVE-2004-2518 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

Access Vector

NETWORK

Access Complexity

LOW

Authentication

NONE

Confidentiality Impact

PARTIAL

Integrity Impact

NONE

Availability Impact

NONE

CVE References

Description

Tags

Link

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](https://exchange.xforce.ibmcloud.com/text/html)
[text/html](#)

[XF gattaca-language-path-disclosure\(16700\)](#)

SecurityTracker.com Archives - Gattaca Server Multiple Input Validation Bugs Let Remote Users Deny Service, Determine System Information, and Conduct Cross-Site Scripting Attacks

[Exploit](#)
[securitytracker.com](https://securitytracker.com/text/html)
[text/html](#)

[SECTrack 1010703](#)

404 - File or directory not found.

[www.gattaca-server.com](http://www.gattaca-server.com/text/html)
[text/html](#)
Inactive Link **Not Archived**

[CONFIRM www.gattaca-server.com/cgi-bin/yabb/YaBB.pl?board=gattaca_discussion;action=display;num=1091194176;start=0#0](http://www.gattaca-server.com/cgi-bin/yabb/YaBB.pl?board=gattaca_discussion;action=display;num=1091194176;start=0#0)

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](https://exchange.xforce.ibmcloud.com/text/html)
[text/html](#)

[XF gattaca-null-path-disclosure\(16699\)](#)

No Description Provided	Exploit www.osvdb.org	OSVDB 7923
	Inactive Link Not Archived	
Page not found - CVE.report	Patch members.lycos.co.uk text/plain Inactive Link Not Archived	MISC members.lycos.co.uk/r34ct/main/Gattaca%20Server%202003.txt
Secunia - Advisories - Gattaca Server 2003 Multiple Vulnerabilities	Exploit Vendor Advisory web.archive.org text/html	SECUNIA 12071
Gattaca Server 2003 Multiple Path Disclosure Vulnerabilities	Exploit cve.report (archive) text/html	BID 10729
No Description Provided	Exploit www.osvdb.org	OSVDB 7922
	Inactive Link Not Archived	

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Geeos Team	Gattaca Server 2003	1.1.10.0	All	All	All
Operating System	Geeos Team	Gattaca Server 2003	1.1.10.0	All	All	All
cpe:2.3:o:geeos_team:gattaca_server_2003:1.1.10.0:****:***:						
cpe:2.3:o:geeos_team:gattaca_server_2003:1.1.10.0:****:***:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023 |

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](#).

