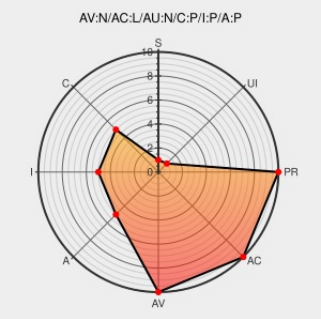
CVE-2001-0689

Published on: 08/29/2001 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:20 PM UTC

CVE-2001-0689

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Virus Control System from Trend Micro contain the following vulnerability:

Vulnerability in TrendMicro Virus Control System 1.8 allows a remote attacker to view configuration files and change the configuration via a certain CGI program.

CVE-2001-0689 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Neohapsis Archives - Bugtraq - [SNS Advisory No.29] Trend Micro Virus Control System(VCS) Unauthenticated CGI Usage Vulnerability - From snsadv@lac.co.jp	Vendor Advisory, web.archive.org, text/html, Inactive Link, Not Archived	BUGTRAQ 20010607 [SNS Advisory No.29] Trend Micro Virus Control System(VCS)

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Trend Micro	Virus Control System	1.8	All	All	All
Application	Trend Micro	Virus Control System	1.8	All	All	All

cpe:2.3:a:trend_micro:virus_control_system:1.8:*:*:*:*:*:*:*:

cpe:2.3:a:trend_micro:virus_control_system:1.8:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→