



CVE-2004-0128

- MITRE
- NVD
- CVE.ORG
- JSON API
- Print: PDF

Summary

CVE	CVE-2004-0128
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2004-03-03 05:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	PHP remote file inclusion vulnerability in the GEDCOM configuration script for phpGedView 2.65.1 and earlier allows remot

Risk And Classification

Primary CVSS: v2.0 7.5 from nvd@nist.gov

AV:N/AC:L/Au:N/C:P/I:P/A:P

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:N/AC:L/Au:N/C:P/I:P/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Phpgedview	Phpgedview	2.52.3	All	All	All

Application	Phpgedview	Phpgedview	2.60	All	All	All
Application	Phpgedview	Phpgedview	2.61	All	All	All
Application	Phpgedview	Phpgedview	2.61.1	All	All	All
Application	Phpgedview	Phpgedview	2.65	All	All	All
Application	Phpgedview	Phpgedview	2.65.1	All	All	All

Vendor Declared Affected Products						
Source	Vendor	Product	Version	Platforms		
CNA	Na	N/a	affected n/a	Not specified		

References		
Reference	Source	Link
Secunia - Advisories - PhpGedView Arbitrary File Inclusion Vulnerabilities	af854a3a-2127-422b-91ae-364da2661108	secunia.com
www.osvdb.org/3769	af854a3a-2127-422b-91ae-364da2661108	www.osvdb.org
IBM X-Force Exchange	af854a3a-2127-422b-91ae-364da2661108	exchange.xforce.ibm
PhpGedView [GED_File]_conf.php Remote File Include Vulnerability	af854a3a-2127-422b-91ae-364da2661108	www.securityfocus.c
SecurityFocus	af854a3a-2127-422b-91ae-364da2661108	www.securityfocus.c
SourceForge.net: File Release Notes and Changelog	af854a3a-2127-422b-91ae-364da2661108	sourceforge.net
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.