CVE-2005-1666

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

Summary

CVE	CVE-2005-1666
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-05-18 04:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Multiple buffer overflows in Orenosv HTTP/FTP Server 0.8.1 allow remote authenticated users to cause a denial of service

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	Orenosv	Orenosv Http Ftp Server	All	All	All	All

Vendor Declared Affected Products

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

References

Reference
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
SecuriTeam.com ™ - Orenosv HTTP/FTP Server Multiple Buffer Overflows
www.osvdb.org/16166
Orenosv HTTP/FTP Server FTP Command Buffer Overflow Lets Remote Users Crash the Server and HTTP SSI Buffer Overflow May Let Loc
IBM X-Force Exchange
IBM X-Force Exchange
Secunia - Advisories - Orenosv HTTP/FTP Server Buffer Overflow Vulnerabilities
Orenosv HTTP/FTP Server
SIG^2 G-TEC - Orenosv HTTP/FTP Server Buffer Overflow Vulnerabilities
www.osvdb.org/16165
Orenosv HTTP/FTP Server CGISSI.EXE Remote Buffer Overflow Vulnerability
Orenosv HTTP/FTP Server FTP Commands Remote Buffer Overflow Vulnerability
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 registred 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**