



CVE-2010-2075

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

Summary

CVE	CVE-2010-2075
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-06-15 14:04:26 UTC
Updated	2026-04-29 01:13:23 UTC
Description	UnrealIRCd 3.2.8.1, as distributed on certain mirror sites from November 2009 through June 2010, contains an externally ir

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: CWE-20 | 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	Unrealircd	Unrealircd	3.2.8.1	All	All	All

Vendor Declared Affected Products				
Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified
References				
Reference				Source
www.unrealircd.com/txt/unrealsecadvistory.20100612.txt				af854a3a-2
Full Disclosure: Fw: [irc-security] UnrealIRCd 3.2.8.1 backdoored on official ftp and site				af854a3a-2
oss-security - Re: CVE request: UnrealIRCd 3.2.8.1 source code contained a backdoor allowing for remote command execution				af854a3a-2
osvdb.org/65445				af854a3a-2
UnrealIRCd Backdoor Unauthorized Access Vulnerability				af854a3a-2
UnrealIRCd Backdoor Security Issue and User Authentication Buffer Overflow - Advisories - Community				af854a3a-2
Unreal IRCd 3.2.8.1 Remote Downloader/Execute Trojan				af854a3a-2
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH				af854a3a-2
Full Disclosure: Re: Fw: [irc-security] UnrealIRCd 3.2.8.1 backdoored on official ftp and site				af854a3a-2
Gentoo Linux Documentation -- UnrealIRCd: Multiple vulnerabilities				af854a3a-2
CVE Program record				CVE.ORG
NVD vulnerability detail				NVD
No vendor comments have been submitted for this CVE.				
There are currently no legacy QID mappings associated with this CVE.				