CVE-2008-6737

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

Summary

CVE	CVE-2008-6737
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-04-21 18:30:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	Crysis 1.21 and earlier allows remote attackers to obtain sensitive player information such as real IP addresses by sending

Risk And Classification

Primary CVSS: v2.0 7.8 from nvd@nist.gov

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

Problem Types: CWE-200 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

None

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ea	Crysis	1.1	All	All	All

Application	Ea	Crysis	1.2	All	All	All
Application	Ea	Crysis	All	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
Crysis Disconnect Packet Information Disclosure - Secunia Advisories - Vulnerability Intelligence - Secunia.com	af854a3a-2127-422b-91ae-
IBM X-Force Exchange	af854a3a-2127-422b-91ae-
Crysis 'keyexchange' Packet Information Disclosure Vulnerability	af854a3a-2127-422b-91ae-
aluigi.altervista.org/adv/crysislog-adv.txt	af854a3a-2127-422b-91ae-
osvdb.org/46260	af854a3a-2127-422b-91ae-
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.