



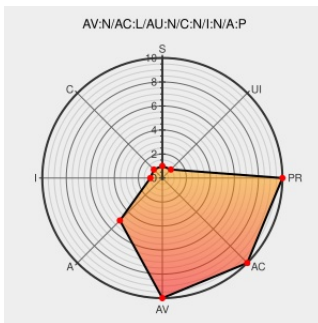
Last Modified on: 03/23/2021 11:28:09 PM UTC

CVE-2004-1395

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF 

Certain versions of [Contract Jack](#) from [Monolith Productions](#) contain the following vulnerability:

The Littech engine, as used in (1) Contract Jack 1.1 and earlier, (2) No one lives forever 2 1.3 and earlier, (3) Tron 2.0 1.042 and earlier, (4) F.E.A.R. (First Encounter Assault and Recon), and possibly other games, allows remote attackers to cause a denial of service (connection refused) via a UDP packet that causes recvfrom to

generate a return code that causes the listening loop to exit, as demonstrated using zero byte packets or packets between 8193 and 12280 bytes, which result in conditions that are not "Operation would block."

CVE-2004-1395 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
[Full-Disclosure] Socket unreacheable in the Lithtech engine (new protocol)	Exploit Patch web.archive.org text/html Inactive Link Not Archived	🌐 FULLDISC 20041213 Socket unreacheable in the Lithtech engine (new protocol)
	Exploit Patch aluigi.altervista.org text/plain	🔗 MISC aluigi.altervista.org/adv/lihtsock-adv.txt

Secunia - Advisories - Lithtech Engine UDP Datagram Denial of Service Vulnerability	web.archive.org text/html	 SECUNIA 13446
Monolith Lithtech Game Engine Remote Denial Of Service Vulnerability	Exploit cve.report (archive) text/html	 BID 11902
'Socket unreachaeable in the Lithtech engine (new protocol)' - MARC	marc.info text/html	 BUGTRAQ 20041213 Socket unreachaeable in the Lithtech engine (new protocol)
[Full-disclosure] F.E.A.R. 1.01 likes lithsock	web.archive.org text/html Inactive Link Not Archived	 FULLDISC 20051021 F.E.A.R. 1.01 likes lithsock
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	 XF lithtech-engine-communication-dos(18456)
Secunia - Advisories - F.E.A.R. Lithtech Engine Denial of Service and Format String Vulnerabilities	web.archive.org text/html	 SECUNIA 17317

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Monolith Productions	Contract Jack	1.1	All	All	All
Application	Monolith Productions	Contract Jack	1.1	All	All	All
Application	Monolith Productions	No One Lives Forever 2	1.0.004	All	All	All
Application	Monolith Productions	No One Lives Forever 2	1.3	All	All	All
Application	Monolith Productions	No One Lives Forever 2	1.0.004	All	All	All
Application	Monolith Productions	No One Lives Forever 2	1.3	All	All	All
Application	Monolith Productions	Tron	2.0.1.0	All	All	All
Application	Monolith Productions	Tron	2.0.1.42	All	All	All
Application	Monolith Productions	Tron	2.0.1.0	All	All	All
Application	Monolith Productions	Tron	2.0.1.42	All	All	All

cpe:2.3:a:monolith_productions:contract_jack:1.1:*:*:*:*:*:

cpe:2.3:a:monolith_productions:contract_jack:1.1:*:*:*:*:*:

cpe:2.3:a:monolith_productions:no_one_lives_forever_2:1.0.004:*:*:*:*:*:

cpe:2.3:a:monolith_productions:no_one_lives_forever_2:1.3:*:*:*:*:*:

cpe:2.3:a:monolith_productions:no_one_lives_forever_2:1.0.004:*:*:*:*:*:

cpe:2.3:a:monolith_productions:no_one_lives_forever_2:1.3:*****:	
cpe:2.3:a:monolith_productions:tron:2.0.1.0:*****:	
cpe:2.3:a:monolith_productions:tron:2.0.1.42:*****:	
cpe:2.3:a:monolith_productions:tron:2.0.1.0:*****:	
cpe:2.3:a:monolith_productions:tron:2.0.1.42:*****:	
No vendor comments have been submitted for this CVE	
← Previous ID	Next ID→