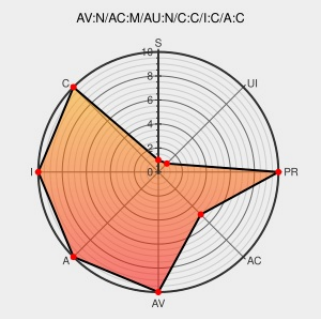
CVE-2007-5247

Published on: 10/06/2007 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:37 PM UTC

CVE-2007-5247

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of First Encounter Assault Recon from Monolith Productions contain the following vulnerability:

Multiple format string vulnerabilities in the Monolith Lithtech engine, as used by First Encounter Assault Recon (F.E.A.R.) 1.08 and earlier, when Punkbuster (PB) is enabled, allow remote attackers to execute arbitrary code or cause a denial of service (daemon crash) via format string specifiers in (1) a PB_Y packet to the YPG server on UDP port 27888 or (2) a PB_U packet to UCON on UDP port 27888, different vectors than CVE-2004-1500. NOTE: this issue might be in Punkbuster itself, but there are insufficient details to be certain.

CVE-2007-5247 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 9.3 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
No Description Provided	osvdb.org Inactive Link Not Archived	OSVDB 45531
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF fear-punkbuster-format-string(36900)
SecurityReason - Format string in F.E.A.R. 1.08 through PB	securityreason.com text/html	SREASON 3197
	Exploit	MISC aluigi.altervista.org/adv/fearfspb-adv.txt

	Exploit aluigi.altervista.org text/plain	MISC aluigi.altervista.org/adv/fearfspb-adv.txt
No Description Provided	osvdb.org Inactive Link Not Archived	OSVDB 45530
Luigi Auriemma	Exploit aluigi.org text/html	MISC aluigi.org/poc/fearfspb.zip
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20071001 Format string in F.E.A.R. 1.08 through PB

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	First Encounter Assault Recon	All	All	All	All

cpe:2.3:a:monolith_productions:first_encounter_assault_recon:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→