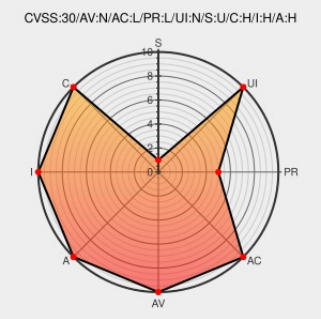
CVE-2017-16666

Published on: 01/05/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:38 PM UTC

CVE-2017-16666

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



Certain versions of Xplico from Xplico contain the following vulnerability:

Xplico before 1.2.1 allows remote authenticated users to execute arbitrary commands via shell metacharacters in the name of an uploaded PCAP file. NOTE: this issue can be exploited without authentication by leveraging the user registration feature.

CVE-2017-16666 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 9 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Xplico Remote Code Execution	Exploit Third Party Advisory www.rapid7.com text/html	MISC www.rapid7.com/db/modules/exploit/linux/http/xplico_exec

Xplico Remote Code Execution ≈ Packet Storm	Exploit Third Party Advisory VDB Entry packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/145639/Xplico-Remote-Code-Execution.html
Xplico – Xpico 1.2.1: Xplico vulnerability	Vendor Advisory www.xplico.org text/html	CONFIRM www.xplico.org/archives/1538
Security Onion: Security Advisory for Xplico 1.2.0	Third Party Advisory blog.securityonion.net text/html	CONFIRM blog.securityonion.net/2017/11/security-advisory-for-xplico-120.html
Xplico - Remote Code Execution (Metasploit) - Linux remote Exploit	Exploit Third Party Advisory VDB Entry www.exploit-db.com Proof of Concept text/html	EXPLOIT-DB 43430
Advisory | Xplico Unauthenticated Remote Code Execution CVE-2017-16666 – Pentest Blog	Exploit Third Party Advisory pentest.blog text/html	MISC pentest.blog/advisory-xplico-unauthenticated-remote-code-execution-cve-2017-16666/

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Xplico	Xplico	All	All	All	All
Application	Xplico	Xplico	All	All	All	All

cpe:2.3:a:xplico:xplico:*:*:*:*:*:*:*:*:

cpe:2.3:a:xplico:xplico:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report