



[Full Disclosure](#) mailing list archives



[By Date](#) [By Thread](#)



CVE-2020-2656 - Low impact information disclosure via Solaris xlock

From: Marco Ivaldi <marco.ivaldi () mediaservice net>

Date: Wed, 15 Jan 2020 13:50:25 +0000

Dear Full Disclosure,

Please find attached an advisory for the following vulnerability, fixed in Oracle's Critical Patch Update (CPU) of January 2020:

"A low impact information disclosure vulnerability in the setuid root xlock binary distributed with Solaris may allow local users to read partial contents of sensitive files. Due to the fact that target files must be in a very specific format, exploitation of this flaw to escalate privileges in a realistic scenario is unlikely."

Regards,

--

Marco Ivaldi, Offensive Security Manager
CISSP, OSCP, QSA, ASV, OPSA, OPST, OWSE, LA27001, PRINCE2F
@Mediaservice.net S.r.l. con Socio Unico
<https://www.mediaservice.net/>

Attachment: [2020-01-solaris-xlock.txt](#)

Description: 2020-01-solaris-xlock.txt

Sent through the Full Disclosure mailing list

<https://nmap.org/mailman/listinfo/fulldisclosure>

Web Archives & RSS: <http://seclists.org/fulldisclosure/>

[By Date](#) [By Thread](#)

Current thread:

CVE-2020-2656 - Low impact information disclosure via Solaris xlock *Marco Ivaldi (Jan 17)*



Nmap Security
Scanner

Ref Guide

Install Guide

Docs

Download

Nmap OEM

Npcap packet
capture

User's Guide

API docs

Download

Npcap OEM

Security Lists

Nmap Announce

Nmap Dev

Full Disclosure

Open Source Security

BreachExchange

Security Tools

Vuln scanners

Password audit

Web scanners

Wireless

Exploitation

About

About/Contact

Privacy

Advertising

Nmap Public Source
License

