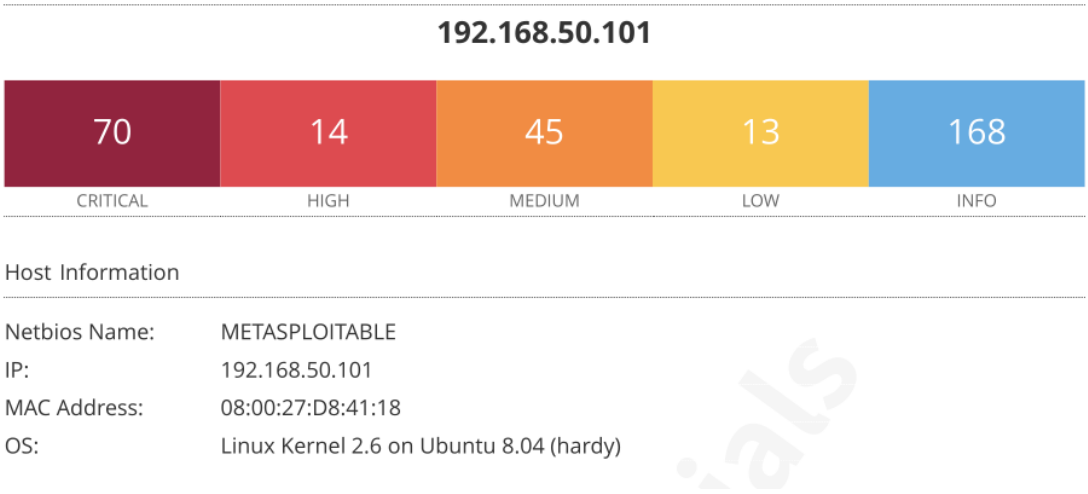
“RELAZIONE S5L4”

Attraverso l’utilizzo dell’applicativo “**NESSUS**” abbiamo eseguito la scansione delle vulnerabilità dell’indirizzo IP 192.168.50.101 ricevendo il seguente rapporto.



Da questo possiamo evincere che il :

NOME NET BIOS = METASPLOITABLE

INDIRIZZO IP = 192.168.50.101

MAC ADDRESS = 08:00:27:D8:41:18

SISTEMA OPERATIVO = LINUX KERNEL 2.6 ON UBUNTU 8.04

Presenta circa 70 VULNERABILITA’ critiche alle quali urge il bisogno di risoluzione

Nel punto sottostante andremo a prendere in esempio una delle criticità e ad effettuare una possibile soluzione :

156016 - Apache Log4Shell RCE detection via Path Enumeration (Direct Check HTTP)

Synopsis

The remote web server is affected by a remote code execution vulnerability.

Description

The remote web server is affected by a remote code execution vulnerability via a flaw in the Apache Log4j library. The vulnerability is due to the processing of unsanitized input sent to a logging function. A remote, unauthenticated attacker can explolit this, via a web request to execute arbitrary code with the permission level of the running Java process.

See Also

https://logging.apache.org/log4j/2.x/security.html

https://www.lunasec.io/docs/blog/log4j-zero-day/

Solution

Upgrade to Apache Log4j version 2.15.0 or later, or apply the vendor mitigation.

Upgrading to the latest versions for Apache Log4j is highly recommended as intermediate versions / patches have known high severity vulnerabilities and the vendor is updating their advisories often as new research and knowledge about the impact of Log4j is discovered. Refer to https://logging.apache.org/log4j/2.x/security.html for the latest versions.

Qui abbiamo un problema di aggiornamento del software

Quindi la solzione e agiornare il software alla versione 2.15.0 o successive