

Cómo Detectar La Vulnerabilidad GHOST



La vulnerabilidad GHOST es una vulnerabilidad de [desbordamiento de búfer](#) que puede ser fácilmente explotada de forma local y remota, lo que hace que sea bastante peligrosa. Esta vulnerabilidad lleva el nombre de la **función** `gethostbynameb`, la cual es

usada en la explotación.

Los atacantes utilizan [vulnerabilidades de desbordamiento](#) de búfer como éste por el envío de paquetes específicos de datos a un sistema vulnerable. El ataque permite al atacante ejecutar código arbitrario y tomar el control de la máquina vulnerable de la víctima.

Esta vulnerabilidad expone a una gran cantidad de usuarios, ya que radica en la librería glibc (GNU). Afortunadamente existen [métodos](#) y aplicaciones para **detectar la vulnerabilidad GHOST**.

¿Qué Puedo Hacer Sobre La Vulnerabilidad GHOST?

Al igual que con cualquier vulnerabilidad, la mejor manera de **acabar con la vulnerabilidad GHOST** es identificar los sistemas vulnerables, priorizar el proceso de parcheo basado en la prioridad, y desplegar parches. Debe mantener un inventario actualizado de los dispositivos, sistemas operativos y aplicaciones en su red para que pueda conocer aquellos dispositivos que son vulnerables.

AlienVault Unified Security Management (USM), también te puede ser de gran ayuda. USM ofrece el descubrimiento de **sistemas vulnerados**, evaluación de vulnerabilidades, detección de amenazas y el seguimiento del comportamiento, todo desde la misma consola; además de actualizaciones semanales de análisis de riesgos desarrollados por el equipo de investigación de seguridad de **AlienVault Labs**.

USM puede escanear la red para identificar los **sistemas vulnerables con GHOST**, por lo que es fácil identificar sistemas que necesitan ser parcheados y dar prioridad para solucionados.



The screenshot displays the 'VULNERABILITIES' section of the AlienVault USM interface, specifically the 'THREAT DATABASE' tab. It shows search results for the keyword 'CVE-2015-0235'. The results are presented in a table with columns for ID, RISK, DEFINED ON, THREAT FAMILY & SUMMARY, and CVE ID. The table lists several entries related to local security checks on various Linux distributions like Debian, Ubuntu, Red Hat, and CentOS.

SEARCH RESULTS FOR THIS CRITERIA					
START DATE	END DATE	KEYWORDS	CVE ID	FAMILY	RISK FACTOR
All	All	CVE-2015-0235	All	All	All
ID	RISK	DEFINED ON	THREAT FAMILY & SUMMARY	CVE ID	
703142	High	2015-02-02 10:04:58	Debian Local Security Checks - NOSUMMARY	CVE-2012-4656 CVE-2014-6040 CVE-2014-7817 CVE-2015-0235	
840077	High	2015-02-02 10:04:58	Ubuntu Local Security Checks - NOSUMMARY	CVE-2015-0235	
871307	High	2015-02-02 10:04:58	Red Hat Local Security Checks - NOSUMMARY	CVE-2015-0235	
871308	High	2015-02-02 10:04:58	Red Hat Local Security Checks - NOSUMMARY	CVE-2015-0235	
882107	High	2015-02-02 10:04:58	CentOS Local Security Checks - NOSUMMARY	CVE-2015-0235	
882108	High	2015-02-02 10:04:58	CentOS Local Security Checks - NOSUMMARY	CVE-2015-0235	
882109	High	2015-02-02 10:04:58	CentOS Local Security Checks - NOSUMMARY	CVE-2015-0235	

USM no sólo puede identificar los sistemas vulnerables, sino que también puede ayudar a detectar los intentos de explotación de la vulnerabilidad.