CERT-GH SECURITY ADVISORY

CERT-GH
Ghana Computer Emergency Response Team

GNU C Library vulnerability

CERT GH REFERENCE #: **CERT-ADV10001032016**
Date Discovered: 16th February 2016

Severity: High
Status: Pending

System(s) Affected	All Ubuntu Platforms
Description	GNU C Library could be made to crash or run programs if it received specially crafted network traffic. It was discovered that the GNU C Library incorrectly handled receiving responses while performing DNS resolution. A remote attacker could use this issue to cause the GNU C Library to crash, resulting in a denial of service, or possibly execute arbitrary code. One of the most dangerous attack vectors that use this library is the code that parses responses for DNS requests. An example of a possible attack vector: An attacker redirects the victim's machine to a domain he controls. • The victim's machine sends a request to the attacker's DNS server. • The attacker's DNS server sends a response that exploits the vulnerability and effectively allows malicious code to run on the victim's machine. • For a long time, this vulnerability has been known as a bug, but researchers only recently realized the implications of the problem
Impact	The cost of a Distributed Denial of Service (DDoS) attack can continue to impact on the targeted organization long after the event has been dealt with. It is not just the disruption to the public interface, which is damaging enough to any organization that conducts a substantial volume of its business online. Loss of revenues while services and systems are unavailable to customers are compounded by the cost of rectifying the crisis and long-term damage to the business's reputation In some cases an organization might even submit to extortion from the hackers, effectively paying a ransom to rid itself of the problem – until the next strike from another hacker source.
Solutions	The problem can be corrected by updating your system to the following package version: Ubuntu 15.10: libc6 2.21-0ubuntu4.1 Ubuntu 14.04 LTS:

	libc6 2.19-0ubuntu6.7 Ubuntu 12.04 LTS: libc6 2.15-0ubuntu10.13
References & Further Information	http://www.ubuntu.com/usn/usn-2900-1/ https://wiki.ubuntu.com/Security/Upgrades