UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00230

LINUX WEB SERVERS HIT BY IMUNIFY360 BUG

DATE ISSUED: 1st December 2021

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

The security platform for Linux-based websites and webservers, CloudLinux, contains a high severity (rated 8.2/10 CVSS) PHP deserialization bug known as Imunify360 leaving the servers open to Remote Code Execution (RCE) and potential full takeover.

BREAKDOWN

The security platform itself is intended to allow users to manage configuration of various settings to implement real-time website protections and server security using advanced firewalls, intrusion detection and protection, anti-malware scanning and automatic kernel patch updates through a single panel integration. The Imunify360 bug, currently tracked as CVE-2021-219565, is found in the Ai-Bolit scanning function which is normally used for site administrators to search for malicious code, malware and potential vulnerabilities. The signature detection mechanisms used in the Ai-Bolit function that looks for common obfuscators, using a handler to de-obfuscate and pull essential code which contains a call to the unserialize function. This function lacks input sanitization checks which would allow an attacker to execute arbitrary code during this key step. This function is installed by default with root level privileges.

REMEDIATION STEPS

- Upgrade to the latest version to apply the appropriate security patches.

REFERENCES & RESOURCES

Threatpost https://threatpost.com/linux-web-servers-imunify360-bug/176508/
Linux Security https://linuxsecurity.com/news/security-vulnerabilities/imunify360-bug-leaves-linux-web-servers-open-to-code-execution-takeover