



Author: Harshal Harekar

Date: 14/10/2025

Chained Exploit on Web Server

Findings

A critical vulnerability was identified in UnrealIRCd version 3.2.8.1 running on [Host: 192.168.18.138]. This version contains a hardcoded backdoor that allows unauthenticated remote attackers to execute arbitrary commands with root privileges. The exploit was successfully demonstrated by gaining a root shell through Metasploit.

Remediation

- Immediately replace UnrealIRCd 3.2.8.1 with a secure, verified version.
- Audit all externally sourced software for integrity.
- Implement strict network segmentation and firewall rules to isolate IRC services.