SARVOTTAM VULNERABILITY REPORT

CERPHIAN

Cerphian Scan Report Summary

Target: www.sarvottamnoida.com

IP Address: 68.178.155.222

Scan Date: 2024-10-19

Scan Duration: 0.077s latency

Total Ports Scanned: 1000

Open Ports: 10

Filtered Ports: 990 (no response)

Open Ports and Services Detected

Port	State	Service	Version
21/tcp	Open	FTP	Pure-FTPd
22/tcp	Open	SSH	OpenSSH 8.0 (protocol 2.0)
80/tcp	Open	HTTP	Apache httpd
110/tcp	Open	POP3	Dovecot pop3d
143/tcp	Open	IMAP	Dovecot imapd
443/tcp	Open	HTTPS	Apache httpd (SSL)
587/tcp	Open	SMTP	Exim smtpd 4.96.2
993/tcp	Open	IMAPS	Unknown
995/tcp	Open	POP3S	Unknown
3306/tcp	Open	MySQL	MySQL 5.5.5-10.6.19-MariaDB-cll-lve

Vulnerabilities Identified

1. OpenSSH 8.0 (CVE-2023-38408)

- **Severity:** 9.8 (Critical)
- **Description:** This vulnerability allows an attacker to exploit a flaw in the OpenSSH implementation, leading to potential unauthorized access.
- **References:** CVE-2023-38408

2. MySQL 5.5.5-10.6.19-MariaDB (Multiple CVEs)

- **Severity:** Up to 10.0 (Critical)
- **Description:** Various vulnerabilities affecting MySQL and MariaDB that can be exploited to gain unauthorized access or execute arbitrary code.
- **References:**
  - CVE-2012-2750
  - CVE-2016-9843
  - More CVEs listed in the detailed output.

3. Exim SMTP (CVE-2023-42116)

- **Severity:** 8.1 (High)
- **Description:** A vulnerability that allows remote attackers to bypass restrictions in the Exim mail server.
- **References:** CVE-2023-42116

4. Dovecot (POP3/IMAP)

- **Severity:** Various CVEs identified (details not provided in the output).
- **Description:** Dovecot is known to have vulnerabilities that may lead to unauthorized access or service disruption.

Risk Assessment

Overall Risk Level: High

1. **Critical Vulnerabilities:**
    - The presence of OpenSSH 8.0 with a critical CVE and several high-severity vulnerabilities in the MySQL service poses a significant risk to the server's security and data integrity.
2. **Service Exposure:**
    - Multiple open ports for sensitive services (FTP, SSH, HTTP, SMTP, MySQL) increase the attack surface. Each open service is a potential entry point for attackers.
3. **Exploitability:**
    - Given the critical and high-severity vulnerabilities identified, there is a real possibility for exploitation, especially if these services are accessible from the internet without proper security measures (e.g., firewalls, intrusion detection systems).
4. **Potential Impact:**
    - If exploited, these vulnerabilities could lead to unauthorized access, data breaches, and loss of service, significantly affecting the organization’s operations and reputation.

Recommendations

1. **Immediate Patching:**
    - Upgrade OpenSSH and MySQL/MariaDB to the latest stable versions to mitigate known vulnerabilities.
2. **Firewall Configuration:**
    - Limit access to critical ports (especially SSH and MySQL) only to trusted IP addresses.
3. **Intrusion Detection:**
    - Implement an intrusion detection/prevention system (IDPS) to monitor traffic and block suspicious activities.

4. **Regular Security Audits:**
    - Conduct regular vulnerability assessments and penetration testing to identify and mitigate new threats.
5. **Backup and Recovery:**
    - Ensure that backups are regularly taken and that recovery procedures are tested.

This report highlights significant security concerns that require immediate attention. Prioritizing these recommendations will help mitigate the risk associated with the identified vulnerabilities.