VIBIDSOFT HACK RECOVERY · INCIDENT REPORT

Website compromise risk: exposed credentials and open mail relay

Professional services company · public website (PHP) with a WordPress blog

SAMPLE · ANONYMISED

1. Summary

A full security review of the organisation's website found **no active malware**, but it found a critical weakness that attackers could abuse at any time. Two forgotten backup copies of the contact-form script contained **hard-coded credentials for a cloud email service**. Because they would send mail to any address a visitor typed, they worked as an **open spam relay** through the organisation's own email account.

The credentials were revoked, the files and an outdated mail library were removed, the server rules were hardened and the contact form was rebuilt. Every WordPress file was verified against official checksums. The site stayed online throughout.

Organisation	[redacted] (professional services, India)
Systems in scope	Main website (PHP), WordPress blog, database export, hosting account, DNS / CDN settings
Recovery tier	Business Recovery (equivalent)
Overall severity	**Critical (exposed credentials, open relay)**
Data exposure	No evidence that customer data was accessed. Cloud email sending history was reviewed for abuse.
Status	Closed. Monitoring in place.

2. Timeline

WHEN	WHAT HAPPENED
Day 1, morning	Review started. Snapshot of all website files, the blog database export and server logs taken before any change.
Day 1, midday	WordPress core and every plugin compared with official checksums; about 5,500 uploaded files checked for hidden code. All matched; no web shells found.
Day 1, afternoon	Critical finding: two backup contact-form scripts with hard-coded cloud email credentials, reachable from the web. Owner informed immediately.
Day 1, afternoon	**Contained:** access key deactivated and deleted by the owner; both scripts and the outdated mail library removed from the server; requests to them now refused.

Day 1, evening	Server rules hardened; public error logs blocked; new contact form with bot protection deployed and tested.
Day 2	Clean-up of leftover files, orphaned admin records and old scripts; scheduled tasks moved to a server cron; report issued.

3. Findings

#	FINDING	SEVERITY	ACTION
1	Cloud email credentials hard-coded in two backup scripts that would send mail to any visitor-supplied address (open relay)	**Critical**	Key revoked; files deleted
2	Old contact form with no bot protection, no validation and raw visitor HTML in emails	**High**	Replaced
3	Server error logs readable from the web, revealing server paths	**Medium**	Blocked and removed
4	Outdated mail library with known vulnerabilities, used only by the backup scripts	**Medium**	Removed
5	Outdated slider plugin with known cross-site scripting issues	**Medium**	Direct access blocked; kept by owner decision
6	Blog loaded a script from a third-party domain	**Low**	Now self-hosted, patched version
7	Orphaned administrator records for deleted users; leftover old files	**Low**	Cleaned up

4. How an attacker could have got in

> The weak point was not a clever exploit. It was **forgotten files**: backups left on the live server years earlier, with working credentials inside. Anyone who found them could send spam as the organisation, damage its email reputation and run up cloud charges. Automated scanners look for exactly these file names.

5. What we changed

- Cloud email access key deactivated and deleted; sending history reviewed.
- Backup scripts, outdated mail library, old configuration copies and leftover files removed (kept offline as evidence).
- Server rules: HTTPS and one canonical host; directory listings off; backups, logs, dumps and config files refused; attack query strings blocked; security headers added.
- Blog: XML-RPC and user enumeration blocked; no script execution in uploads.
- New contact form: server-side bot verification, honeypot, rate limit, strict validation, escaped email content.
- Scheduled tasks moved from page-load triggers to a server cron job.

- File permissions tightened on configuration files.

6. Recommendations

- Update or remove the outdated slider plugin.
- Keep backups off the web server; never store credentials in website files.
- Two-factor authentication on hosting, DNS, registrar and every admin account.
- Monthly access and ownership check (Search Console, DNS, hosting, admin users).
- Ongoing protection: a Shield plan with a named engineer and tested monthly updates.

This is an anonymised sample of a real Vibidsoft engagement, published with the owner's permission. Names, account details, addresses and file paths are removed. Times are shown as day and part of day. Vibidsoft · www.vibidsoft.com/hacked-website-repair · inquiry@vibidsoft.com