ramsac
the secure choice

Patch. Protect. Prevent.

What is patching and why does it matter?

A patch is a software update to fix bugs, improve performance, or most importantly, close security vulnerabilities. Unpatched systems are a major target for cybercriminals. Applying patches promptly is crucial to prevent breaches. Failing to apply patches promptly leaves known weaknesses exposed, giving cybercriminals an easy way in. Threat actors actively search for these gaps, often exploiting them faster than organisations can respond.

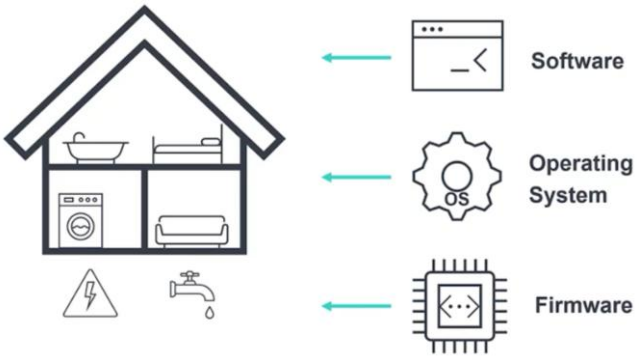
What needs patching?

- **Operating Systems** (Windows, macOS, iOS, etc.)
- **Software/Applications** (e.g. Chrome, Microsoft Office, Adobe)
- **Firmware** (drivers, embedded software)
- **Network & Edge Devices** (e.g. firewalls, access points, VPN gateways)
- **Servers and Infrastructure** (cloud or on-premise)

All require ongoing maintenance to stay secure and functional.

Using the house analogy:

- OS is the structure/foundation
- Software is the furniture and appliances
- Firmware is the wiring and plumbing



Understanding Vulnerabilities

A vulnerability is a known flaw in software or code that could be exploited. These flaws can:

- **Allow unauthorised access**
- **Enable code execution (e.g. ransomware)**
- **Give control of a device to a hacker**

Vulnerability reports have more than doubled over five years, with nearly 11,000 already identified in 2025. This surge underlines the urgent need for active vulnerability management. Even large, well-trusted software's get flaws and open vulnerabilities, emphasising that your data too is at risk.

- Adobe products: 6,155 vulnerabilities reported to date
- Google Chrome: 3,602 vulnerabilities

Core parching principles

To minimise risk, organisations should follow these key principles:

1. **Know your assets:** Maintain a full inventory of all devices, including shadow IT and IoT (e.g. smart speakers, printers).
2. **Patch all layers:** Not just OS—include third-party apps and firmware.
3. **Prioritise severity:** Focus first on high-risk vulnerabilities using a risk-based approach.
4. **Automate patching:** Where possible, to reduce human error and speed up response times.
5. **Report and review:** Ensure patches are actually being applied. Monitor for devices that fall out of patch cycles.

For organisations working towards **Cyber Essentials** certification, patching becomes even more important. To remain compliant, all critical updates must be applied within 14 days of release.

Checklist: How Secure Is Your Organisation's Patching?

If you can answer 'yes' to the following, you're in a strong position:

- ✓ Do you have an up-to-date asset inventory?
- ✓ Are vulnerabilities tracked across all systems?
- ✓ Are operating systems, software, and firmware kept current?
- ✓ Is patching automated or scheduled regularly?
- ✓ Is patching success tracked and exceptions reviewed?

Clients on our supported IT service benefit from automated workstation patching, with critical operating system updates typically deployed within days of release. Firmware and driver patching is also available, planned carefully to minimise disruption. Our Vulnerability Management as a Service (VMaaS) offers clear visibility of security risks and includes automated patching for key third-party apps like browsers and Adobe tools. We can also manually patch network devices such as firewalls and access points where needed.

Patching is non-negotiable for organisations serious about security. The threat landscape is growing, and cybercriminals move fast. Patching needs to be proactive, prioritised, and visible.

Find out more

Contact us for more information for how ramsac can help your organisations cybersecurity and how you can make the secure choice.

Tel: **01483 412 040** email: **info@ramsac.com**