

Preparing for a ‘vulnerability patch wave’

Organisations must act now to prepare for a wave of patches that will address decades of technical debt.

Whether they are technology producers and vendors, or consumers and operators, all organisations have ‘technical debt’; a backlog of technical issues – that is both expensive and time-consuming – as a result of prioritising short-term gains over building resilient products.

Artificial Intelligence, when used by sufficiently-skilled and knowledgeable individuals, is showing the ability to exploit this technical debt at scale and at pace across the technology ecosystem. As a result, the NCSC expects there will be a ‘forced correction’ to address this technical debt across all types of software, including open source, commercial, proprietary and software as a service.

This is why we are encouraging all organisations to prepare now for when a ‘patch wave’ arrives; a rush of software updates that will need to be applied across the technology stack to address the disclosure of new vulnerabilities.

Prioritise external attack surfaces

All organisations must take steps to identify and minimise their internet-facing (and other externally-exposed) attack surfaces as soon as is possible. As we’ve argued for some time, you should [prioritise technologies on your perimeter](#) and then work inwards covering cloud instances and on-premises environments. By doing this, organisations can reduce the risk that latent vulnerabilities pose when they become known and exploited by attackers.

Where organisations cannot apply updates across their entire environment, they should prioritise applying updates to their external attack surfaces. Where capacity extends beyond the external attack surface, organisations should prioritise critical security systems.

It is also important for organisations to realise that patching alone will **not** always suffice; some technical debt may be present in ‘end of life’ or legacy technology that is out of support, and so can’t receive updates. In such instances, organisations will need to replace technologies, or bring them back within support, especially where it presents an *external* attack surface.

Prepare to patch quickly, more often, and at scale

Building on the principles contained within our [Vulnerability Management guidance](#), organisations should make plans to deploy software security updates quickly, more frequently, and at scale, including across their supply chains. We are expecting an influx of updates to address vulnerabilities across all severities, and expect a number to be critical.

The NCSC recommends that:

- where automatic secure ‘hot patching’ is available (that is, patching that doesn’t involve service disruption), this should be enabled as a priority
- where automatic updates are available (including for embedded devices), this should be enabled to reduce the workload on support teams
- where neither of the above are available, organisations will need to ensure that processes and risk appetites support frequent and scaled-updating, noting the operational trade-offs around disruption and safety critical systems. A risk-prioritised approach such as the [Stakeholder Specific Vulnerability Categorisation \(SSVC\) system](#) can be used to prioritise installing the updates

However, should a critical vulnerability be under active exploitation (especially one affecting an internet-facing system), then it is essential to accelerate the update process. Organisations can refer to the NCSC’s new guidance on [‘Responding to active exploitation of vulnerabilities’](#) for more information.

To summarise, you should put in place a policy to ‘update by default’ where you always apply software updates as soon as possible, and ideally automatically. This should be at the core of your update management process, but we recognise that it may not apply in some circumstances (such as for safety-critical systems or operational technology).

Beyond software updates

Patching alone won't address the [systemic problems that my previous blogs have addressed](#). I've appealed to technology producers and vendors to ensure systemic technical security debt is minimised by including - where appropriate - memory safety and containment technologies such as [CHERI](#) and others.

Similarly, for consumers and operators, a focus on cyber security fundamentals to raise resilience and to reduce the impact of breaches should be a priority. This includes adopting and fully implementing [Cyber Essentials](#), or the [Cyber Assessment Framework](#) for organisations operating essential services (such as energy, healthcare, transport, digital infrastructure and government).

For organisations facing elevated threats, the NCSC has also recently produced guidance on:

- [Privileged access workstations \(PAWs\)](#)
- [Cross-domain approach and architecture](#)
- [Cyber resilience through observability and threat hunting](#)

Prepare for the patch wave now

In conclusion, the NCSC advises all organisations, irrespective of size, to plan and prepare for the vulnerability patch wave. A good place to start is by reading the NCSC's updated [Vulnerability Management guidance](#). For larger organisations, we also recommend working to [gain assurance from your supply chains](#) both commercial and open source, so that they are prepared to navigate any required response.

Ollie Whitehouse
CTO, NCSC

WRITTEN BY



Ollie Whitehouse
Chief Technology Officer (CTO), NCSC

PUBLISHED

1 May 2026

PART OF BLOG

Inside the NCSC