National Cyber Security Centre Guidance on Vulnerability Management

1. PUT IN PLACE A POLICY TO UPDATE BY DEFAULT

- □ **Apply updates as soon as possible, and ideally automatically.**
- □ **Put in place a policy to update by default, where you always apply software updates as soon as possible, and ideally automatically.**

  Different Types of Update Considerations
  - □ Some separate the security updates from feature updates, while others combine them.
  - □ Sometimes you can only install the latest update if you have installed a previous one. Multi-version upgrades are more likely to have unintended side effects than single updates.
  - □ Vendors may publish advisories for some vulnerabilities, but also 'silently' update others, without public acknowledgement. Missing an update could mean you also miss these silent updates, heightening the risk to your organisation.
- □ **Rolling Out Considerations**
  - □ Vendors carry out their own quality assurance testing of these updates and once they release them, you should also test on your own systems. This doesn't have to slow down the rollout.
  - □ A phased rollout also allows you to carry out 'live testing' of the estate against the security update.
  - □ As a system owner, set up your communications preferences so that you receive the latest updates as soon as they are available. You should also make sure you have the required licences.
  - □ It's better to stay within the application development rules of the platform – don't try and 'reinvent the wheel'.
  - □ You should use a supported OS that has a cloud platform with an auto-update service.
  - □ Employ infrastructure as code (IaC). The most reliable way to automate is to replace the running image or code with the updated version, rather than having to update it.
  - □ Automation is key to easing the burden.
  - □ If you are using removable media, the removable media should be checked for viruses before installing.
- □ **Best-practice Timescales**
  - □ Internet-facing services and software - **Update within 5 days**
  - □ Operating system and applications - **Update within 7 days**
  - □ Internal/air-gapped service and software - **Update within 14 days**
- □ **Updating when Exploitation is Rife**
  - □ The above timelines are for business-as-usual updates, but there will be times when a vulnerability is discovered and attackers are scanning or attacking the internet at scale to find victims before they update. In these cases, the timelines above are too long and it is essential to to speed up the update process.
  - □ Also be ready to deploy additional vendor updates in the days immediately following the discovery of a new vulnerability.
  - □ Note that if a vulnerability affecting an internet-facing service is being actively exploited in the wild, you should investigate your exposure and check for signs of compromise before applying any update, even if the exposure was brief.
  - □ Recommended Exploitation Sources
    - □ The vendor advisory will include information about the vulnerability and any mitigations. It may also include indicators of compromise, scripts and other support.
    - □ CISA's Known Exploited Vulnerabilities Catalog

4. THE ORGANISATION MUST OWN THE RISKS OF NOT UPDATING

- □ **There may sometimes be legitimate reasons not to update. The decision not to is a senior-level risk decision, and should be considered in the wider context of organisational risk management policy and practice.**
- □ The organisation's risk management structures and staff need to be aware of the risk the organisation has chosen to tolerate at the present time.
- □ **Considerations for Owning The Risk of Not Updating**
  - □ identify and monitor the systems, services, cloud infrastructure, mobile devices, hardware and software in your estate.
  - □ Risk-based prioritisation depending on your organisation's risk assessment and referenced against the CISA Known Exploited Vulnerabilities Catalog or threat intelligence feeds.
  - □ **You shouldn't make decisions based purely on a single severity score, such as CVSS.**
  - □ Potential impact on the system or service
  - □ Potential for reputational damage to the system, service or your organisation.
  - □ Direct cost, such as replacing obsolete systems.
  - □ Availability and cost of a short-term fix.
  - □ Availability and cost of skilled resources to carry out the work.
  - □ Cost of incident response and recovery, including any fines imposed in a worst-case scenario.
  - □ Once a decision is made, record the reasons behind it, and ensure any remaining risk is considered in your organisation's overall risk management framework.

2. IDENTIFY YOUR ASSETS

- □ **Understanding what systems and software you have on your technical estate, who is responsible for what, and which vulnerabilities are present.**
- □ Agree on the tasks which the security and IT system maintainers carry out. This should include the cadence and nature for reporting on detected vulnerabilities, the time and effort system maintainers should allocate to correcting issues, and agreeing the appropriate priority of an IT incident.
- □ **Asset Discovery**
  - □ identify and monitor the systems, services, cloud infrastructure, mobile devices, hardware and software in your estate.
  - □ Asset discovery, and cataloguing and managing your estate as it changes over time, is a continual process. Automating these processes means you can focus on the results.
- □ **Obsolete and Extended-Support Products**
  - □ The best remediation here is to migrate to a supported product before it reaches end of life. Where this isn't possible, you will need to manage the risks associated with obsolete products.
  - □ The NCSC recommends that once a product is out of mainstream support you migrate to a supported version.
- □ **Configuration Management**
  - □ The NCSC has device security guidance to help organisations choose and configure devices securely, and one of the most effective security controls are application allow lists.
  - □ We recommend that you automate configuration audits, and that they provide coverage across your whole estate. Where possible, any new system should be deployed using infrastructure as code and configuration as code, to reduce the risks of misconfiguration and make remediation at scale easy.

3. CARRY OUT ASSESSMENTS BY TRIAGING AND PRIORITISING

- □ **To manage your attack surface, you should carry out vulnerability assessments across the entire estate at least every month.**
- □ More mature organisations should consider even more regular assessments, particularly for services that are externally reachable.
- □ **Scanning**
  - □ A regular scanning regime is essential to make you aware of the risks your organisation may face.
  - □ The NCSC has guidance on how to choose, implement and use automated vulnerability scanning tools.
- □ **Vulnerability Disclosure**
  - □ If you develop software or run systems, you should also consider setting up a process to allow security researchers to report to you any vulnerabilities they have found.
  - □ The NCSC Vulnerability Disclosure Toolkit is designed to make setting up a disclosure process easy.
- □ **Triaging Vulnerabilities That Can't or Won't be Immediately Mitigated**
  - □ Sometimes installing the latest version of the affected software might not fix the reported vulnerability or misconfiguration, or there may not even be an update to address the issue.
  - □ With sensible controls, such as making sure that decommissioning continues, it's perfectly rational to not update.
  - □ While the vulnerability assessment software or vendor advisory may provide a severity rating for the finding, it's essential that you consider business impact and risk for your organisation.
- □ **Choosing Not to Update**
  - □ Sometimes an organisation may assess that the risks of automatically updating are too high. Where this is the case, the system should be added to an 'exception list' where updates go through any safety testing your organisation requires.
  - □ **The Triage Process**
    - □ Where no update is available whatever the reason, you will need a process to triage and prioritise fixes.
    - □ Consolidate all the issues and apply the same triage and prioritisation process so that system owners have full visibility to manage issues accordingly.
    - □ Your triage process should first group all similar findings together, or findings that require the same mitigation.

      Once grouped, they should then be divided into three categories: issues to fix, acknowledge, or investigate.

5. VERIFY AND REGULARLY REVIEW YOUR VM PROCESS

- □ **Vulnerability management processes should be actively verified and always evolving.**
- □ **Put in place a feedback loop to help with this.**
- □ Improvements could include reducing the update timescales, or ensuring asset discovery and management scans are completed and audited more frequently.
- □ **Verification / Regularly Review**
  - □ include a verification process to make sure that where a vulnerability has been fixed using a reconfiguration or mitigation, you have verified that the vulnerability is no longer present.
  - □ If the mitigation is only a temporary workaround, you will need to keep monitoring it.

VulnCheck

Source: National Cyber Security Centre