Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

**TLP: AMBER**

# Advisory: 2018-07-26 - Organisations within the health sector impacted with WannaCry

Over recent weeks, the Australian Cyber Security Centre (ACSC) has become aware of media devices within a small number of organisations in the health sector being infected with WannaCry ransomware. This specific type of ransomware variant was first detected in May 2017, spreading across 150 different countries in just two days and affecting over 200,000 organisations, causing significant disruption to critical services including the health sector in the United Kingdom.

The ransomware leverages publicly-known vulnerabilities in Microsoft Windows, with appropriate patches available from Microsoft since March 2017 (Microsoft Security Bulletin MS17-010). Additionally, Microsoft has released patches for older, unsupported Microsoft operating systems on 13 May 2017. If you are running older systems, these patches should be applied immediately.

The ACSC strongly advises organisations ensure their devices are up to date with the latest patches so they are not vulnerable to these types of threats.

## Recommendations

The ACSC recommends that partners undertake the following actions:

- Apply MS17-010 patches as soon as possible to prevent infection by this ransomware.
- If unable to patch then consider disabling SMBv1.
- Review and consider applying ASD Essential Eight mitigation strategies.
- Review logs for unusual SMB traffic.
- Ensure that important data is backed up to an offline location.

Additionally, Microsoft have released advice and a special hotfix for Windows XP, Server 2003, and Windows 8 RTM.

- https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/.
- https://blogs.technet.microsoft.com/mmpc/2017/05/12/wannacrypt-ransomware-worm-targets-out-of-date-systems/.
- http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598.

## Feedback

The ACSC welcomes any feedback you may have with regard to this publication and/or the services we provide – asd.assist@defence.gov.au; or 1300 292 371 (1300 CYBER 1).

TLP: AMBER

# Traffic light protocol

The following table lists the classification levels used in the traffic light protocol (TLP) and describes the restrictions on access and use for each classification level.

| TLP classification | Restrictions on access and use |
|---|---|
| RED | Access to and use by your ACSC security contact officer(s) only.<br><br>You must ensure that your ACSC security contact officer(s) does not disseminate or discuss the information with any other person, and you shall ensure that you have appropriate systems in place to ensure that the information cannot be accessed or used by any person other than your ACSC security contact officer(s). |
| AMBER | Restricted internal access and use only.<br><br>Subject to the below, you shall only make AMBER publications available to your employees on a 'need to know basis' strictly for your internal processes only to assist in the protection of your ICT systems.<br><br>In some instances you may be provided with AMBER publications which are marked to allow you to also disclose them to your contractors or agents on a need-to-know basis—strictly for your internal purposes only to assist in the protection of your ICT systems. |
| GREEN | Restricted to closed groups and subject to confidentiality.<br><br>You may share GREEN publications with external organisations, information exchanges, or individuals in the network security, information assurance or critical network infrastructure community that agree to maintain the confidentiality of the information in the publication. You may not publish or post on the web or otherwise release it in circumstances where confidentiality may not be maintained. |
| WHITE | Not restricted.<br><br>WHITE publications are not confidential. They contain information that is for public, unrestricted dissemination, publication, web-posting or broadcast. You may publish the information, subject to copyright and any restrictions or rights noted in the information. |
| NOT CLASSIFIED | Any information received from ACSC that is not classified in accordance with the TLP must be treated as AMBER classified information, unless otherwise agreed in writing ACSC. |