Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

TLP:WHITE

2019-009: Securing Unprotected Network and Data Services

The Australian Cyber Security Centre (ACSC), the cyber defensive component of the Australian Signals Directorate (ASD), has observed a large number of unprotected network and database/storage services hosted on Australian Internet Protocol (IP) address ranges.

This exposure may lead to data contained in these services being compromised. The ACSC urges organisations to check their externally facing internet services and ensure appropriate access controls and protections are in place.

Details

As part of the ACSC, the Australian Internet Security Initiative (AISI) operates as a public-private partnership where Australian internet providers and other network owners voluntarily work with the ACSC to help protect their customers and/or themselves from cyber security threats.

The program helps to reduce malicious software (malware) infections and service vulnerabilities occurring on Australian IP address ranges. Daily email reports are sent to internet providers identifying IP addresses on their networks observed as being infected by malware or potentially vulnerable to exploitation. Internet providers are encouraged to use the AISI data to identify and inform affected customers about their malware infection or service vulnerability. This includes providing advice to customers on how they can remove the malware or secure the vulnerable service.

Over recent weeks, the ACSC has received a number of reports about cyber security incidents that could have been prevented if the affected party had signed up to the **free** AISI program and actioned the alert data it provides.

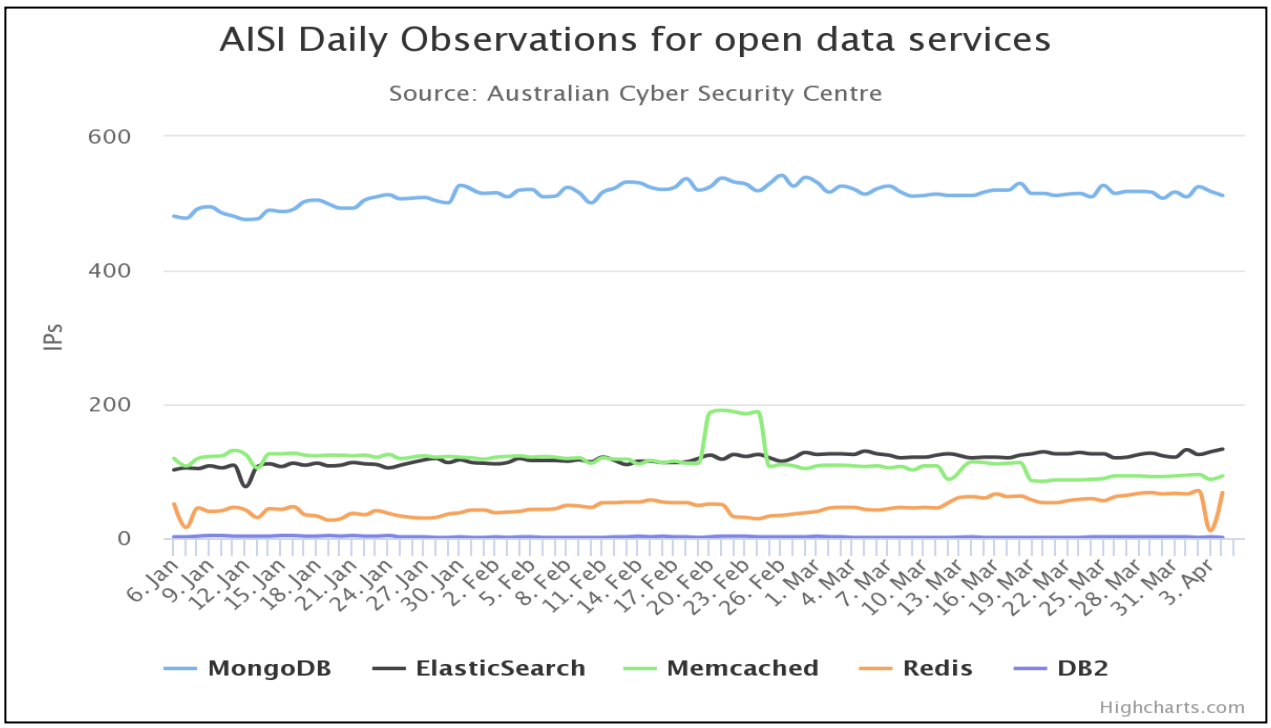
The web-facing services reported through the AISI are often vulnerable because they have inadequate authentication and access control processes in place. Malicious actors are known to exploit these types of vulnerable services in order to commit further cyber attacks such as:

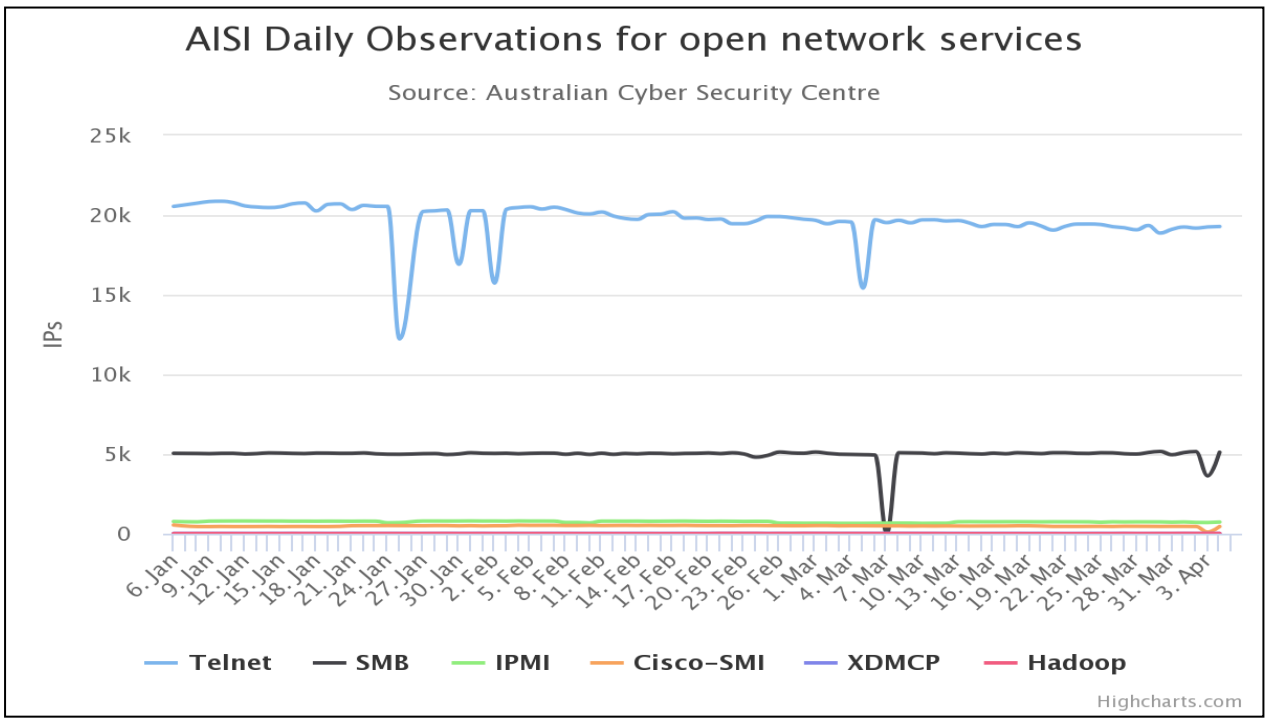
- Ransomware
- Theft and/or modification of data and intellectual property
- Business disruption
- Denial of Service attacks
- Advanced Persistent Threat (APT) entry into key business sectors
- Other harmful activities to either the service owner or other interest users.

The two graphs below illustrate some key vulnerable services identified through the AISI during the first quarter of 2019. Note that there are a lot of other vulnerable services that are detected through AISI monitoring, but they do not appear in these charts.

For example, the first graph shows that there were around 500 open Mongo Databases and 100 ElasticSearch Databases detected each day across Australia, while the second graph indicates that there were around 20,000 open network services that were potentially vulnerable to exploitation.

TLP:WHITE


AISI Daily Observations for open data services
Source: Australian Cyber Security Centre
IPs
600
400
200
0
6. Jan
9. Jan
12. Jan
15. Jan
18. Jan
21. Jan
24. Jan
27. Jan
30. Jan
2. Feb
5. Feb
8. Feb
11. Feb
14. Feb
17. Feb
20. Feb
23. Feb
26. Feb
1. Mar
4. Mar
7. Mar
10. Mar
13. Mar
16. Mar
19. Mar
22. Mar
25. Mar
28. Mar
31. Mar
3. Apr
MongoDB
ElasticSearch
Memcached
Redis
DB2
Highcharts.com


AISI Daily Observations for open network services
Source: Australian Cyber Security Centre
IPs
25k
20k
15k
10k
5k
0
6. Jan
9. Jan
12. Jan
15. Jan
18. Jan
21. Jan
24. Jan
27. Jan
30. Jan
2. Feb
5. Feb
8. Feb
11. Feb
14. Feb
17. Feb
20. Feb
23. Feb
26. Feb
1. Mar
4. Mar
7. Mar
10. Mar
13. Mar
16. Mar
19. Mar
22. Mar
25. Mar
28. Mar
31. Mar
3. Apr
Telnet
SMB
IPMI
Cisco-SMI
XDMCP
Hadoop
Highcharts.com

TLP:WHITE

Recommendations

All Australian businesses and organisations should ensure they have implemented strong user authentication and access controls on their databases and network infrastructure, including across all available environments (i.e. development, test, staging, pre-production and production).

The ACSC recommends the following actions:

- Ensure the service interface is not exposed to the internet if it is not required
- Ensure the service interface only listens on localhost/127.0.0.1 if it does not require remote access
- Ensure service administration interface is not exposed on the internet
- Use Virtual Private Network (VPN) connection where applicable
- Implement proper access control including IP whitelisting, user account, and role-based access control
- Use least privileged user accounts, e.g. read-only access accounts for auditing and reporting purposes
- Use Data Loss Prevention (DLP) and Intrusion Prevention System (IPS)/Intrusion Detection System (IDS)
- Strong password policy for both user and service accounts
- Use Multi Factor Authentication wherever possible[1]
- Implement Network Segmentation and Segregation[2]
- Retain audit and access logs
- Regularly monitors logs for suspicious activities
- Use Transport Layer Security (TLS) to secure communication in accordance with the Australian Government Information Security Manual (ISM) wherever possible[3]
- Review product vendors' security guidelines
    - AWS S3[4]
    - MongoDB[5]
    - Redis[6]
    - DB2[7]
    - ElasticSearch[8]
    - Memcached[9]
    - Hadoop[10]
    - Cisco-SMI[11]
    - Contact your product vendor for relevant security documentation if the service is not listed here.
- Report data breaches to the ACSC for assistance
- If a data breach has resulted from an unprotected service, you may be required to report this to the Office of the Australian Information Commissioner (OAIC). To determine whether you are required to report a data breach, please read about the Notifiable Data Breaches Scheme (NDB) [12] on the OAIC website.

TLP:WHITE

Contact details

Australian customers with questions regarding this advice should contact the ACSC on 1300 CYBER1 (1300 292 371) or asd.assist@defence.gov.au

You are eligible to participate in the AISI if you have been assigned Australian IP address ranges and are solely responsible for the management of these ranges. If you would like to participate in the AISI, please send an email to asd.assist@defence.gov.au with the following information:

- the IP address ranges associated with your network (preferably in CIDR format)
- an email address to send the daily AISI email reports to (ideally a generic email address rather than an individual email address)
- a direct contact number(s) and email address to discuss AISI operational matters
- the name by which you want your company to be listed on the AISI website.

References

1. https://cyber.gov.au/business/publications/multi-factor-authentication-pdf/
2. https://cyber.gov.au/government/publications/network-segmentation-and-segregation-pdf/
3. https://cyber.gov.au/government/publications/australian-government-information-security-manual-ism/ Page 135
4. https://docs.aws.amazon.com/AmazonS3/latest/dev/s3-access-control.html
5. https://docs.mongodb.com/manual/security/
6. https://redis.io/topics/security
7. https://www.ibm.com/support/knowledgecenter/en/SSEPGG_11.1.0/com.ibm.db2.luw.admin.sec.doc/doc/c0021804.html
8. https://www.elastic.co/guide/en/elasticsearch/reference/current/configuring-security.html
9. https://github.com/memcached/memcached/wiki/ConfiguringServer#networking
10. https://hadoop.apache.org/docs/stable/hadoop-project-dist/hadoop-common/SecureMode.html
11. https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170214-smi
12. https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme

TLP:WHITE

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. 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. 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. 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. 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. 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.