AUSCERT

– AUSTRALIAN PIONEER CYBER EMERGENCY RESPONSE TEAM

Membership Services Overview

HERE'S HOW WE CAN HELP YOU

Our unique range of services means we can be your main point of contact when dealing with data security incidents.

INCIDENT SUPPORT

Our Incident Support service assists your organisation to detect, interpret and respond to attacks from across the globe. Whether you're facing an incident or just need guidance, our team is here to help you.

As a member, you will have access to our highly skilled team of security analysts and developers with SANS GIAC and other certifications who are available through email, Slack or our 24/7 Member Hotline.

- **24/7 Member Hotline** – Our team is on call 24/7 to assist with urgent incidents.
- **Email** – Contact our team during normal business hours (AEST)
- **Slack** – Join our team and other AusCERT members in conversation.

Our team follow well-defined protocols in order to obtain a resolution and satisfactory outcome with you. As such, we recommend that our members incorporate contacting AusCERT into their Incident Response Plan. The Incident Support service is provided remotely, and the level of support is on a best effort basis.

AusCERT triages the incidents reported according to criticality from our assessment of the incident as it is presented to our analysts. Criticality follows the generally accepted four (4) tiers with levels that are mapped to business impact: Event, Incident, Serious Incident, Critical Incident.

Escalation of an incident:

- During office hours AEST we will receive incidents and look at them for response immediately if an email is followed by a phone call.

- Out of office hours using our 24/7 Member Hotline will garner immediate attention to your incident of which a follow-up with an email will be recommended.

Should no phone call be accompanied by your incident request by email, then it is expected that a response from AusCERT will be followed within three (3) business hours. An assessment of criticality will then be looked at with respect to the business impact of the incident to the incident reporter and resources to assist through our service will be allocated with respect to the triage load levels of the day.

Every time we receive new information from your organisation, or from other sources with respect to your incident, AusCERT will reassess the criticality of your incident to match the development of your incident.

For incidents that require analysis of an artefact and response, this is provided for the first three (3) hours of work which is placed under triage. If the incident requires further assistance, based on the scope of the issue we determine if an analyst can be allocated to assist (at cost). If our team is unable to assist further directly (based on availability or the type of incident), we can provide unbiased recommendations of other trusted providers.

PHISHING TAKEDOWN

AusCERT's Phishing Takedown service is designed to assist your organisation with targeted phishing, spear phishing and whaling attacks. If your organisation's brand is used on a phishing web site, or if spear phishing targets your organisation, AusCERT can utilise its worldwide contact network to request removal of the fraudulent web site.

Our team can assist with:

- Hosting takedown - if it is an individual site that is designed with malicious intent
- Domain revocation - if the whole domain is used for malicious intent.

Drawing on our strong international CERT relationships we have a high success rate in delivering phishing takedowns.

When your organisation contacts us with details of a phishing site, our team will investigate to (1) determine if the site's malicious content is due to a vulnerability of a legitimate site and contact the owner, (2) contact hosting provider directly with details regarding the malicious intent of the site and request a take-down and if needed (3) contact the registrar directly and request the takedown.

Please note that AusCERT can only assist with take-downs if there is evidence of phishing or malicious behaviour from the domain. We cannot assist if it is a case of a domain name or website branding that infringes on your organisation's name/brand without any malicious behaviour.

Our team can also assist with general phishing/malicious emails that your organisation receives that target your users. You can send samples through to our team for us to analyse and take action. All members collectively benefit when AusCERT is alerted to these emails as we will add the URLs to the Malicious URL Feed service for members to consume (see page 7).

SECURITY BULLETINS

AusCERT specialises in vulnerability research to deliver members a consistently formatted feed of bulletins across major platforms and vendors streamlining security patching.

Security Bulletins include information that quickly summarises the contents and allows readers to determine important information at a glance. This allows your organisation to easily determine the severity and prioritise your organisational security patching.

AusCERT utilises the **Common Vulnerability Scoring System (CVSS)** which is the industry standard for assessing the severity of security vulnerabilities.

The bulletin content includes **Common Vulnerabilities and Exposures (CVE)** identifiers that relate to the vulnerability for reference, and a suggested resolution to protect against the vulnerability including patch/upgrade and mitigation recommendations.

AusCERT issues two types of bulletins:

- AusCERT Security Bulletins (or 'ASBs')
- External Security Bulletins (or 'ESBs')

ASBs are written in-house, referencing information available that may not have a current coherent source, while ESBs are bulletins written by other vendors that we have summarised and re-released. An ‘ALERT’ flag is also added to the subject line if the contents of the bulletin are time-critical or reference an actively exploited vulnerability.

Security Bulletins are published by AusCERT each business day Security Bulletins are published by AusCERT each business day with content curated and checked to ensure up-to-date information is provided to our members.

More information about the format and content of our Security Bulletins is available from:

https://auscert.org.au/publications/member-information/2017-07-11-auscert-bulletin-formats/

Email Subscriptions

Members can create multiple customised email subscriptions to the Security Bulletins service for specific operating systems and environments that are relevant to your organisation. Bulletins are sent via email immediately as they are published by AusCERT.

- **Organisational** bulletin subscriptions
    - Your organisation can create customised subscriptions for your team/s using an email alias or internal mailing list. This is also useful for people in your organisation who would like to receive security bulletins but do not require a user account.
- **Personal** bulletin subscriptions
    - Every user on the membership account can also create and manage their own bulletin subscription if required.

Security Bulletins are also available via an **RSS Feed** which is provided in the same consistent format.

Daily Bulletin Digest

Alternatively, Members can subscribe to receive the Daily Bulletin Digest. This is a single email issued at the end of each business day that summarises all the bulletins published by AusCERT that day, with hyperlinks to view each bulletin. This provides a quick and easy way to keep across the bulletins that are being issued by AusCERT while still having the ability to view the full bulletin content for those that are relevant to your organisation.

⚠ MEMBER SECURITY INCIDENT NOTIFICATIONS (MSINS)

Member Security Incident Notifications (MSINs) are customised composite security reports that are relevant to your organisation.

MSINs are tailored for your organisation based on your IPs and domains that are nominated on your membership account. They contain a compilation of "security incident reports" as observed by AusCERT through its threat intelligence platforms.

MSINs are issued via email on a daily basis and provide:

- Relevant and timely notifications of threats and incidents
- Details of the threat and recommended mitigation
- Reminders on unresolved incidents and vulnerabilities

Members are only issued with an MSIN if at least one incident report specific to the member's IPs/domains is detected within the past 24-hour period. This also means this if there are no incidents to report, you will not receive an MSIN.

Members may also request to have specific reports 'muted' if they no longer want to be notified about them for a particular IP/domain. More information about the format and content of our Security Bulletins is available from:

https://www.auscert.org.au/publications/2017-06-30-guide-auscert-member-security-incident-

SENSITIVE INFORMATION ALERT

Sensitive Information Alerts provide notification via email when sensitive material is found online by our analyst team which specifically targets your organisation.

The sensitive material typically consists of leaked credentials such as a username in the form of an email address and an authentication string (hash or passwords).

These alerts are based upon the domains that are registered to your organisation which are nominated and verified on your membership account.

Members are only issued with a Sensitive Information Alert if leaked credentials are found by our analyst team. Sensitive Information Alerts are issued via email and will include an encrypted file containing the leaked credentials for your team to analyse and action.

EARLY WARNING SMS

Early Warning SMS alerts are issued by our analyst team when there is a high-impact vulnerability that is of the utmost importance to the security of members which your organisation should consider acting on swiftly.

These alerts are typically in reference to an ongoing malicious campaign targeting members or a high-impact Security Bulletin which identifies remote code execution, has a PoC released or has an exploit in wild affecting members. SMS messages are only sent to the contacts nominated to receive these alerts on your membership account.

These alerts will be sent when such a vulnerability is identified by the analyst team and therefore can be sent 24/7. These alerts are for notification only so that your organisation may take action as required and do not require a response to AusCERT.

MALICIOUS URL FEED

On a day-to-day basis, AusCERT encounters numerous phishing and malware attacks which are analysed and curated in the Malicious URL feed.

This Australian-based feed contains a list of active phishing, malware, malware logging or mule recruitment websites which can be added to your firewall blacklist and SIEM to help prevent compromises to your network.

The feed is updated every five (5) minutes and content is often added during business hours. It is available for two different time periods:

- Previous 24-hour feed
- Previous 7 days feed

It's also split into two separate categories, or an all-inclusive feed, in both txt and xml formats.

- Phishing (txt/xml)
- Malware (txt/xml)
- Combination (txt/xml)

A lot of our members use the API to ingest the feeds into their web proxies etc. on their own schedule, or you could fetch it once a day via the Member Portal if you'd prefer a manual approach. The API key can be generated in the Member Portal and can be used in a pre-populated script in Python, Bash/Curl or Powershell.

Members are encouraged to contribute to the feed by reporting phishing/malicious emails that your organisation receives that target your users. You can send samples through to our team for us to analyse and take action. All members collectively benefit when AusCERT is alerted to these attacks as we will add the URLs to the feed for members to consume.

AUSCERT.ORG.AU

QUESTIONS ABOUT OUR SERVICES OR HOW TO BECOME A MEMBER?

membership@auscert.org.au

AUSTRALIA'S PIONEER
CYBER EMERGENCY RESPONSE TEAM