

## Just One of 734: Australian Defence Contractor Hacked

Article By:

Cameron Abbott

---

A hacker has breached the computer system of an unnamed defence contractor and stolen 30 gigabytes of data, including information on Australia's \$17 billion Joint Strike Fighter program.

The data breach, which the Australian Government publicly disclosed last week, also includes information about Australia's \$4 billion P-8 surveillance plane project, Collins Class submarines and the warships HMAS Canberra and HMAS Adelaide. The Government has emphasised that the stolen data is commercially sensitive but not classified.

The announcement coincides with the release of the Australian Cyber Security Centre's 2017 Threat Report, available [here](#), which reveals that the hack is among 734 cyber incidents affecting private sector systems of national interest and critical infrastructure providers.

In this instance, the hacker had access to data for about 4 months before the breach was discovered in November last year.

In an investigation into the breach, the Australian Signals Directorate (**ASD**) found that the hacker exploited a weakness in the software that had not been updated for 12 months and could have used username-password combinations such as "admin admin" and "guest guest" to access the defence contractor's web portal.

The defence contractor is a small aerospace engineering business with about 50 employees, subcontracted 4 levels down from defence contracts.

The ASD has not yet discovered the identity of the hacker and has not ruled out that it could be a foreign state actor.

Read more [here](#) and [here](#).

*Olivia Coburn also contributed to this article.*

Copyright 2025 K & L Gates

---

Source URL: <https://natlawreview.com/article/just-one-734-australian-defence-contractor-hacked>