# Integrity of thousands of SATCOM devices at risk!

## A Wake-up Call for SATCOM Security

Satellite Communications (SATCOM) play a vital role in the global telecommunications system. IOActive (a leading computer security services provider) evaluated the security posture of the most widely deployed SATCOM terminals. This phase focused on analyzing and reverse engineering the freely and publicly available firmware updates for popular SATCOM technologies manufactured and marketed by Harris, Hughes, Cobham, Thuraya, JRC, and Iridium.

IOActive found that malicious actors could abuse all of the devices within the scope of this study. The vulnerabilities included what would appear to be backdoors, hardcoded credentials, undocumented and/or insecure protocols, and weak encryption algorithms. In addition to design flaws, IOActive also uncovered a number of features in the devices that clearly pose security risks.

Considering the sectors where these products are deployed and the affected vendors, the specific nature of the vulnerabilities IOActive uncovered is of great concern.

Appropriate action to mitigate these vulnerabilities should be taken. Owners and providers should evaluate the network exposure of these devices, implement secure policies, enforce network segmentation, and apply restrictive traffic flow templates (TFT) when possible. Until patches are available, vendors should provide official workarounds in addition to recommended configurations in order to minimize the risk these vulnerabilities pose.

If one of these affected devices can be compromised, the entire SATCOM infrastructure could be at risk. Ships, aircraft, military personnel, emergency services, media services, and industrial facilities (oil rigs, gas pipelines, water treatment plants, wind turbines, substations, etc.) could all be impacted by these vulnerabilities.

For detailed article follow the given link:
http://www.ioactive.com/pdfs/IOActive_SATCOM_Security_WhitePaper.pdf

Ref: http://www.qcert.org/