*** 北米連携センター情報***

2014 年 8 月 27 日

●多数の脆弱性抱える気象衛星

【Nextgov, 2014/08/26】
　商務省監察長官（IG）は、連邦気象衛星プログラムとその契約業者であるレイセオンが、衛星が抱える多数の大きな脆弱性を放置していると批判。
　IG メモによるとシステムの重大な脆弱性は 2012 年当時の 1 万 4486 件から 2 万 3868 件と 60%以上増加しており、指摘されている脆弱性は次世代極軌道気象衛星群「Joint Polar Stellite System」の制御にも影響を与えかねないという。
　米国海洋大気庁（NOAA）は 2010 年から衛星のアップグレードを支援するために地上システムの手直しも開始。しかし 2014 年になるまで地上システムの契約業者に対して、ほとんどのセキュリティコントロールの導入は義務付けていなかった。
　IG メモはこの結果、多くの高リスクな脆弱性がシステム内に存在することになったとしている。
　今回リストアップされた脆弱性には古いソフトウェア・バージョン、修正されないままのバグ、ソフトウェアの設定ミス、過大なアクセス権設定など高リスクとされるものが 9100 件以上あり、この他にもパスワードや監査設定の誤りなどが 3600 件以上見つかった。
　現状ではこれらの多くは後 2 年は手付かずのまま放置されるが、がレイセオンに早急な対応を求めれば一部はすぐにでも修正可能だという。

（参考）本件報道記事

Thousands of Weather Satellite Bugs Won't Be Fixed For Years

The Commerce Department inspector general is blasting a federal climate-satellite program and its supporting contractor, Raytheon, for ignoring tens of thousands of major cyber vulnerabilities.

The weaknesses identified in a new IG memo could impair machines controlling the Joint Polar Satellite System, the nation's next-generation fleet of polar orbiting environmental satellites.

The ground system routes information for the National Oceanic and Atmospheric Administration and the Pentagon, as well as other U.S. and foreign government agencies. NOAA, part of Commerce, manages the information technology system.

The system’s critical vulnerabilities have spiked by more than 60 percent since 2012, increasing from 14,486 security holes to 23,868 holes.

High-Risk Vulnerabilities Persist

In 2010, NOAA began modifying the ground system to support satellite upgrades. But, “until 2014, the program did not require the ground system contractor to begin full implementation of the majority of the security controls for the system," Allen Crawley, assistant IG for systems acquisition and IT security, said in the memo. As a result, "many high-risk vulnerabilities exist within the system."

The government increased Raytheon's now-$1.7 billion contract by $185 million in February to strengthen information security and speed data delivery, company officials said at the time.

The "high-risk vulnerabilities" cited by the IG refer to system weaknesses that make it relatively easy for hackers to gain control of computer components.

"If exploited, these vulnerabilities may make it possible for attackers to significantly disrupt the JPSS mission of providing critical data used in weather forecasting and climate monitoring," Crawley said in the memo, which was released Tuesday.

The satellites controlled by the system track data on oceans, ozone, snow, vegetation and other environmental indicators to help scientists discern changes in the Earth's atmosphere.

But hacker tools are already available on the Web to exploit several of the weaknesses, Crawley noted.

The security problems listed include:

- More than 9,100 instances of high-risk flaws discovered during vulnerability scans, such as outdated software versions, programs that were missing bug fixes, incorrectly configured software, and excessive user privileges for accessing operating systems and software.

- More than 3,600 cases where password and audit settings were misconfigured.
- Unnecessary software applications that need to be removed or disabled.

"The majority of these issues will not be remediated for another two years," Crawley said.

The good news is that some of the vulnerabilities could be mended immediately, if NOAA demanded faster response times from Raytheon.

"Urgent updates to the JPSS ground system were not performed because the program did not require that the ground system contractor remediate vulnerabilities in a timely manner," Crawley said.

NOAA Behind in Applying Security Patches

Agency policies mandate that high-risk issues be fixed within 30 days but in practice, patches were only applied about once a year.

NOAA officials told the IG updates were delayed because of the 2011 liftoff of the program's first satellite -- Suomi National Polar-orbiting Partnership -- and an audit of Raytheon's work.

The agency is on schedule for a launch of a second satellite, JPSS-1, in early 2017, NOAA officials said in June.

Tuesday's memo follows a scathing IG assessment of NOAA's overall satellite security posture in July.

Among the blunders detailed: a hacker stole satellite data from a contractor's personal computer, after which the employee refused to turn over the machine for investigation. Unauthorized smartphone use on critical systems also turned up during the audit.

IG: Security Concerns Justify Special Attention

On Tuesday, Clark Reid, the Commerce IG's legislative and external affairs officer, said in an email significant security concerns involving the Joint Polar Satellite System ground system "justified special and separate attention” in a new memo.

In written remarks responding to a draft memo, NOAA officials said they already are working to address the IG’s findings by, for example, neutralizing the Heartbleed superbug, a vulnerability in widely-used encryption software.

The agency "successfully used expedited processes to enable remediation of Heartbleed in an accelerated manner" between April and June, Vice Adm. Michael Devany, NOAA deputy undersecretary for operations, said in the July 25 correspondence.

Raytheon officials told Nextgov they had not read the report and referred questions to NOAA. Agency officials Tuesday said they had no additional comment.

Source :
http://www.nextgov.com/cybersecurity/2014/08/tens-thousands-weather-satellite-bugs-wont-be-fixed-years/92465/?oref=ng-HPtopstory

以　上