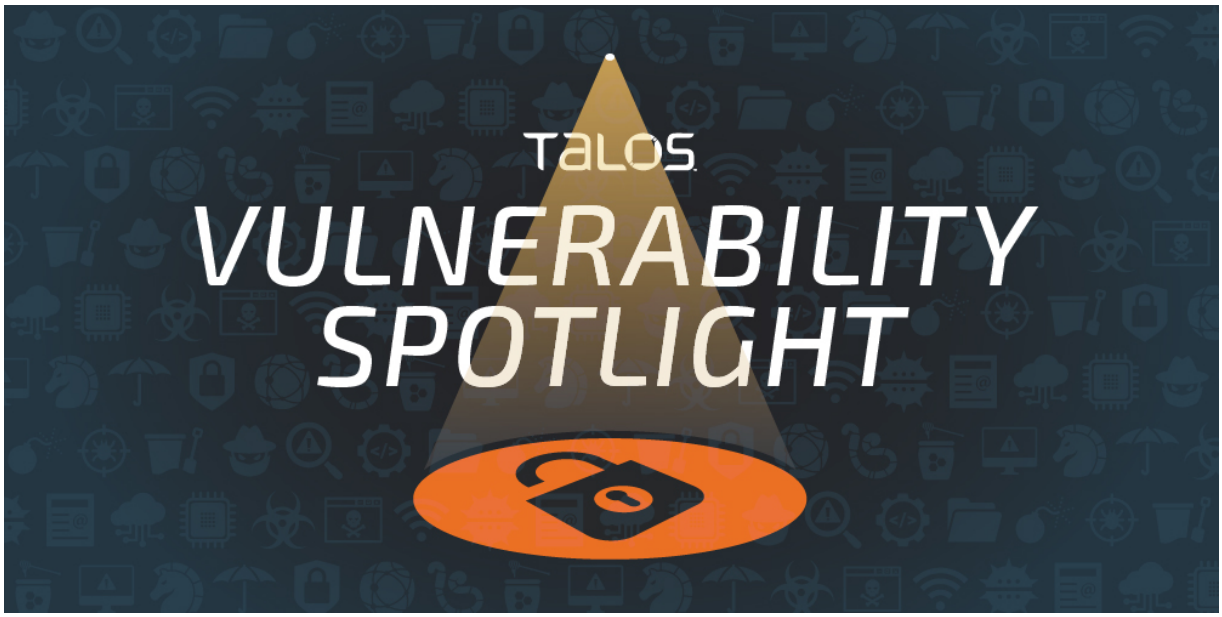
THURSDAY, FEBRUARY 28, 2019

Vulnerability Spotlight: Remote code execution vulnerability in Antenna House Rainbow PDF Office Server Document Converter



Emmanuel Tacheau of Cisco Talos discovered this vulnerability.

EXECUTIVE SUMMARY

Antenna House Rainbow PDF Office Server Document Converter contains a heap overflow vulnerability that could allow an attacker to remotely execute code on the victim machine. Rainbow PDF is a software solution that converts Microsoft Office documents into a PDF. This specific flaw lies in the way the software converts PowerPoint files into PDFs.

In accordance with our coordinated disclosure policy, Cisco Talos worked with Antenna House to ensure that these issues are resolved and that an update is available for affected customers.

VULNERABILITY DETAILS

Antenna House Rainbow PDF Office Server Document Converter getSummaryInformation NumProperties code execution vulnerability (TALOS-2018-0780/CVE-2019-5019)

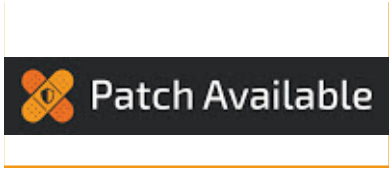
A heap overflow vulnerability exists in the PowerPoint document conversion function of Rainbow PDF Office Server Document Converter V7.0 Pro R1 (7,0,2018,1113). While parsing Document Summary Property Set stream, the getSummaryInformation function is incorrectly checking the

correlation between size and the number of properties in PropertySet packets, causing an out-of-bounds write that leads to heap corruption and consequent code execution.

Read the complete vulnerability advisory here for additional information.

VERSIONS TESTED

Talos tested and confirmed that Antenna House Rainbow PDF, version 7.0 Pro R1 for Linux64 (7,0,2018,1113) is impacted by this vulnerability.



COVERAGE

The following SNORT® rules will detect exploitation attempts. Note that additional rules may be released at a future date and current rules are subject to change pending additional vulnerability information. For the most current rule information, please refer to your Firepower Management Center or Snort.org.

Snort Rules: 49209, 49210

POSTED BY JONATHAN MUNSHAW AT 10:22 AM
LABELS: ANTENNA HOUSE, PDF, RAINBOW PDF, VULNERABILITIES, VULNERABILITY ANALYSIS, VULNERABILITY SPOTLIGHT

SHARE THIS POST

NO COMMENTS:

POST A COMMENT

HOME OLDER POST

SUBSCRIBE TO: POST COMMENTS (ATOM)

Search Blog

SUBSCRIBE TO OUR FEED

Posts

Comments

Subscribe via Email

BLOG ARCHIVE

▼ 2019 (39)

▼ FEBRUARY (19)

Vulnerability Spotlight: Remote code execution vul...

Cisco Talos Honeypot Analysis Reveals Rise in Atta...

Beers with Talos Ep. #47: Privacy, Underwear, and ...

Threat Roundup for Feb. 15 to Feb. 22

Cyber Security Week in Review (Feb. 22)

Combing Through Brushaloader Amid Massive Detectio...

JavaScript bridge makes malware analysis with WinD...

Threat Roundup for Feb. 8 to Feb. 15

Cyber Security Week in Review (Feb. 15, 2019)

Beers with Talos Ep. #46 - Privacy Pwnd: ExileRAT ...

Microsoft Patch Tuesday — February 2019: Vulnerabi...

Vulnerability Spotlight: Adobe Acrobat Reader DC t...

What you can learn from Cisco Talos' new oil pumpj...

Threat Roundup for Feb. 1 to Feb. 8

RECOMMENDED BLOGS

CISCO BLOG

Hotel Pack and IP Phones Make for Easy-Breezy Upgrade

SNORT BLOG

Snort rule update for Feb. 26, 2019

CLAMAV® BLOG

ClamAV is looking for a new team member!