Sign in to view more content

Create your free account or sign in to continue your search

Sign in

Welcome back

Email or phone

Password

Show

Forgot password? Sign in

or

New to LinkedIn? Join now

or

New to LinkedIn? Join now

By clicking Continue to join or sign in, you agree to LinkedIn's User Agreement, Privacy Policy, and Cookie Policy.

LinkedIn

LinkedIn is better on the app

Don’t have the app? Get it in the Microsoft Store.

Open the app
Skip to main content
LinkedIn

- Articles
- People
- Learning
- Jobs
- Games
- Get the app

Join now Sign in

https://mma.prnewswire.com/media/604276/Embedi.jpg?w=800

Exploit available for the dangerous MS Office RCE vuln. called "Skeleton in the closet" CVE2017-11882

- Report this article

Bertin ABENE, CISSP Bertin ABENE, CISSP

Bertin ABENE, CISSP

Sr Information Security Consultant , Founder EOCON | CISSP, SC-100, AWS SA, Project+ I support companies in strengthening their security posture and I animate my cybersecurity community through unique events ;-)

Published Nov 22, 2017
+ Follow

We recently ear about a 17 year old MS Office RCE vulnerability, discovered and named "Skeleton in the closet" by @_embedi_ , a company specializing in cybersecurity solutions for embedded devices.

That vulnerabily is extremelly dangerous because it :

- works with all the Microsoft Office versions released in the past 17 years (including Microsoft Office 365)
- works with all the Microsoft Windows versions (including Microsoft Windows 10 Creators Update)
- is relevant for all the types of architectures
- does not interrupt a user's work with Microsoft Office

- if a document is opened, the vulnerability does not require any interaction with a user to be exploited.

EMBEDI realease a PoC on Github https://github.com/embedi/CVE-2017-11882

Today the exploit have been integrated in Metasploit by Rio @0x09AL. So that, it will be more easy to test how vulnerable you are.

https://github.com/0x09AL/CVE-2017-11882-metasploit

Installation is pretty simple

Copy the cve_2017_11882.rb to :

/usr/share/metasploit-framework/modules/exploits/windows/local/

Copy the cve-2017-11882.rtf to : /usr/share/metasploit-framework/data/exploits/

This module is a quick port to Metasploit and uses mshta.exe to execute the payload. @0x09AL claim that there are better ways to implement this actual module and exploit but will update it as soon as he will have the time.

Another Metasploit module related to CVE2017-11882 have been writed by @goddamnhackers (Realoriginal)

In the meantime, you can start enjoy with this really awesome stuff.

:)

Additional info: https://embedi.com/blog/skeleton-closet-ms-office-vulnerability-you-didnt-know-about.
Like
Comment

- Copy
- LinkedIn
- Facebook
- Twitter

Share
□ 4 6 Comments
See more comments

To view or add a comment, sign in

More articles by this author

No more previous content

- BIG NEWS, the NIST CSF 2.0 has been released. So what ?

  ### BIG NEWS, the NIST CSF 2.0 has been released. So what ?

  Feb 27, 2024

- NIST Cybersecurity Framework version 2.0, what's new ?

  ### NIST Cybersecurity Framework version 2.0, what's new ?

  May 8, 2023

- Tour du "NIST Cybersecurity Framework version 2.0"

  ### Tour du "NIST Cybersecurity Framework version 2.0"

May 8, 2023

- EyesOpenCTF, première compétition en cyber sécurité au Cameroun

  ### EyesOpenCTF, première compétition en cyber sécurité au Cameroun

  Sep 5, 2020

- Tools to expose local port over Internet for demo or pentesting

  ### Tools to expose local port over Internet for demo or pentesting

  Dec 30, 2019

- Conférence EyesOpen Cybersecurity. Que s'est-il passé ?

  ### Conférence EyesOpen Cybersecurity. Que s'est-il passé ?

  Oct 6, 2019

- EyesOpen Security Conference - What's happened ?

  ### EyesOpen Security Conference - What's happened ?

  Oct 6, 2019

- Weaponization: Easily Create a Fully Undetectable (FUD) Empire Powershell MS OFFICE macro

  ### Weaponization: Easily Create a Fully Undetectable (FUD) Empire Powershell MS OFFICE macro

  Jun 7, 2019

- APT Cyber attack workshop using MITRE ATT&CK framework

  ### APT Cyber attack workshop using MITRE ATT&CK framework

  Oct 1, 2018

- When #Wannacry tell you the story of #MS17-010

  ### When #Wannacry tell you the story of #MS17-010

  May 16, 2017

No more next content

See all

Insights from the community

- Computer Maintenance
  How do you customize or configure error logs to suit your needs and preferences?
- Computer Repair
  How do you repair a computer's boot sector with command line tools?
- Computer Repair
  What is the best way to recover data on Mac and Windows devices?
- Computer Science
  What is the difference between a kernel panic and a system crash?
- Computer Literacy
  How do you control file access in a network?
- System Administration
  What causes system hangs and how can you troubleshoot them?
- Operating Systems
  How can you fix corrupted or missing system files?
- Computer Repair
  How do you diagnose computer problems online?
- Technical Support
  How can you troubleshoot a missing or corrupted file error?
- Operating Systems
  What are the best practices for handling bad sectors on a disk?

Show more Show less

Others also viewed

- ### Patch Tuesday sees Microsoft issue 14 bulletins, 4 of which are rated critical

  Ríona Cunningham 9y
- ### September 2021 Blog

  Eric Rintell 3y
- ### Microsoft Issues Out-of-Band Informational Advisory for Zero-Day in MSHTML (CVE-2021-40444)

Ondrej KOVAC 3y

- ### HBCD? why it's an essential tool.

  Omar A. Othman 3y

- ### Description of the security update for Office 2010: May 8, 2018

  Christina Luo 6y

- ### [PowerShell] SCEP - Definition updates

  Badrane DERBAZI 6y

- ### PowerPoint mouse-over event abused to deliver Graphite implants

  Cyber Castrum LLP 2y

- ### Follina - a new vulnerability in Microsoft Office

  Axence Global 2y

- ### FIXING MICROSOFT OFFICE BOOT STRAPPER ERROR

  Ikyagh Raphael Haroun 6y

- ### Patch Tuesday Leaves Outlook Users Outraged

  Shane Kimbrel 8y

Show more Show less

Explore topics

- Sales
- Marketing
- IT Services
- Business Administration

- HR Management
- Engineering
- Soft Skills
- See All

- LinkedIn © 2024
- About
- Accessibility
- User Agreement
- Privacy Policy
- Cookie Policy
- Copyright Policy
- Brand Policy
- Guest Controls
- Community Guidelines
-
  - العربية (Arabic)
  - বাংলা (Bangla)
  - Čeština (Czech)
  - Dansk (Danish)
  - Deutsch (German)
  - Ελληνικά (Greek)
  - **English (English)**
  - Español (Spanish)
  - فارسی (Persian)
  - Suomi (Finnish)
  - Français (French)
  - हिंदी (Hindi)
  - Magyar (Hungarian)
  - Bahasa Indonesia (Indonesian)
  - Italiano (Italian)
  - עברית (Hebrew)
  - 日本語 (Japanese)
  - 한국어 (Korean)
  - मराठी (Marathi)
  - Bahasa Malaysia (Malay)
  - Nederlands (Dutch)
  - Norsk (Norwegian)
  - ਪੰਜਾਬੀ (Punjabi)
  - Polski (Polish)
  - Português (Portuguese)
  - Română (Romanian)
  - Русский (Russian)

- Svenska (Swedish)
- తెలుగు (Telugu)
- ภาษาไทย (Thai)
- Tagalog (Tagalog)
- Türkçe (Turkish)
- Українська (Ukrainian)
- Tiếng Việt (Vietnamese)
- 简体中文 (Chinese (Simplified))
- 正體中文 (Chinese (Traditional))

Language