

LinkedIn and 3rd parties use essential and non-essential cookies to provide, secure, analyze and improve our Services, and to show you relevant ads (including professional and job ads) on and off LinkedIn. Learn more in our [Cookie Policy](#).

Select Accept to consent or Reject to decline non-essential cookies for this use. You can update your choices at any time in your [settings](#).

Accept Reject



Articles

People

Learning

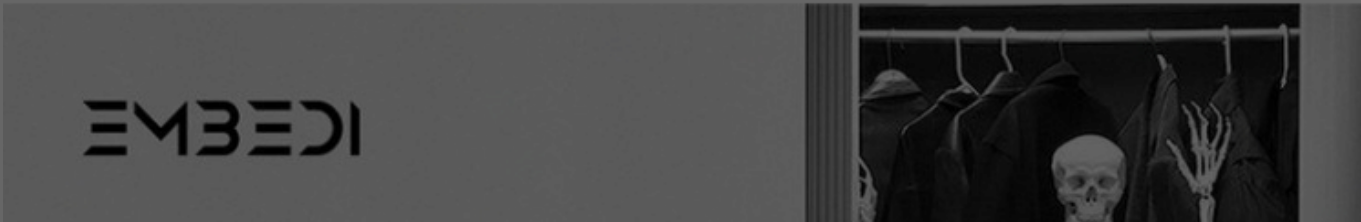
Jobs

Games

Get the app

Join now

Sign in

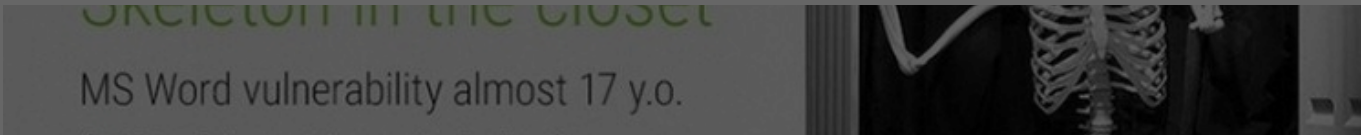


Like

Comment

Share

4 · 6 Comments



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

Bertin ABENE, CISSP

Sr Information Security Consultant at Project+ I support companies in security and I animate my cybersecurity community on LinkedIn.
Published Nov 22, 2017

We recently ear about a 17 year old vulnerability called "Skeleton in the closet" by [@_embedi](#) for embedded devices.

That vulnerability 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

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?

Operating Systems

How can you fix corrupted or missing system files?

Computer Science

What is the difference between a kernel panic and a system crash?

System Administration

What causes system hangs and how can you troubleshoot them?

Show more

Others also viewed

Experts Warn of Stealthy PowerShell Backdoor Disguising as Windows Update

Cyberyami · 2y

Windows Registry and its Forensic significance - Part 2

Akshay Tiwari · 1y

Its Matter in DFIR#2: Prove the Legitimacy of Svchost.exe

Abrar Hussain · 10mo




LINKEDIN

LinkedIn is better on the app

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

Open the app

 LinkedIn and 3rd parties use essential and non-essential cookies to provide, secure, analyze and improve our Services, and to show you relevant ads (including professional and job ads) on and off LinkedIn. Learn more in our [Cookie Policy](#).

Select Accept to consent or Reject to decline non-essential cookies for this use. You can update your choices at any time in your [settings](#).

Show more

Explore topics

Sales

Marketing

IT Services

Business Administration

HR Management

Engineering

Soft Skills

See All



Sign in to view more content

Create your free account or sign in to
continue your search

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](#).

This module is a quick port to Metasploit by [@0x09AL](#) claim that there are better alternatives. I will update it as soon as he will have something better.

Another Metasploit module related to the same exploit by [@goddamnhackers](#) (Realoriginal)

In the meantime, you can start enjoying the exploit :)

Additional info: <https://embedi.com/exploit/0x09AL/0x09AL-MS-Office-Exploit-2017-11882/> [didnt-know-about](#).

See more comments

To view or add a comment, [sign in](#)


More articles by this author

BIG NEWS, the NIST CSF 2.0 has been released. So what?
Feb 27, 2024

NIST Cybersecurity Framework version 2.0, what's new?
May 8, 2023

Tour du "NIST Cybersecurity Framework"
May 8, 2023

See all

 LINKEDIN

LinkedIn is better on the app
Don't have the app? Get it in the Microsoft Store.

Open the app