








Product Solutions Resources Open Source Enterprise Pricing





Sign in


Sign up


 deepinstinct / Lsass-Shtinkering


Public


 Notifications


 Fork 40


 Star 376


 Code


 Issues 1

 Pull requests 2

 Actions

 Projects

 Security

 Insights







 main 







 Go to file

 Code 

	SecurityResearchDeepInstinct	Added link to presentation	7abfb54 · 2 years ago	 4 Commits
	LSASS_Shtinkering	removed unnecessary code		2 years ago
	.gitignore	Initial commit		2 years ago
	LSASS_Shtinkering.sln	Initial commit		2 years ago
	README.md	Added link to presentation		2 years ago

 README



Lsass Shtinkering

New method of dumping LSASS by abusing the Windows Error Reporting service. It sends a message to the service with the ALPC protocol to report an exception on LSASS. This report will cause the service to dump the memory of LSASS.

Prerequisites

The registry value "DumpType" under "HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\LocalDumps" should be set to 2.

Credits







- [Asaf Gilboa](#)

References

- <https://media.defcon.org/DEF%20CON%2030/DEF%20CON%2030%20presentations/Asaf%20Gilboa%20-%20LSASS%20Shtinkering%20Abusing%20Windows%20Error%20Reporting%20to%20Dump%20LSASS.pdf>

About

No description, website, or topics provided.

-  Readme
-  Activity
-  Custom properties
-  376 stars
-  5 watching
-  40 forks
- Report repository



Releases

No releases published

Packages

No packages published

Contributors 2

-  SecurityResearchDeepInstinct
-  ronb-DI

Languages

