LOLBAS Cheatsheet (30/09/2020) (ingenieriainformatica.uniovi.es)

Executables to enable privilege scalation on Windows system

by José Manuel Redondo López

Check the specifics of each executable in https://lolbas-project.github.io/

BINARIES

Program	Possible exploits
At.exe	Execute
Atbroker.exe	Execute
Bash.exe	Execute AWL bypass
Bitsadmin.exe	Alternate data streams Download Copy Execute
CertReq.exe	Download Upload
Certutil.exe	Download Alternate data streams Encode Decode
Cmd.exe	Alternate data streams
Cmdkey.exe	Credentials
Cmstp.exe	Execute AWL bypass
Control.exe	Alternate data streams
Csc.exe	Compile
Cscript.exe	Alternate data streams
Desktopimgdownldr.exe	Download
Dfsvc.exe	AWL bypass
Diantz.exe	Alternate data streams Download
Diskshadow.exe	Dump Execute
Dnscmd.exe	Execute
Esentutl.exe	Copy Alternate data streams Download
Eventvwr.exe	UAC bypass
Expand.exe	Download Copy Alternate data streams
Extexport.exe	Execute
Extrac32.exe	Alternate data streams Download Copy

Program	Possible exploits
Findstr.exe	Alternate data streams Credentials Download
Forfiles.exe	Execute Alternate data streams
Ftp.exe	Execute Download
GfxDownloadWrapper.exe	Download
Gpscript.exe	Execute
Hh.exe	Download Execute
Ie4uinit.exe	Execute
Ieexec.exe	Download Execute
Ilasm.exe	Compile
Infdefaultinstall.exe	Execute
Installutil.exe	AWL bypass Execute
Jsc.exe	Compile
Makecab.exe	Alternate data streams Download
Mavinject.exe	Execute Alternate data streams
Microsoft.Workflow.Compiler.exe	Execute AWL bypass
Mmc.exe	Execute
MpCmdRun.exe	Download Alternate data streams
Msbuild.exe	AWL bypass Execute
Msconfig.exe	Execute
Msdt.exe	Execute AWL bypass
Mshta.exe	Execute Alternate data streams
Msiexec.exe	Execute
Netsh.exe	Execute
Odbcconf.exe	Execute

Program	Possible exploits
Pcalua.exe	Execute
Pcwrun.exe	Execute
Pktmon.exe	Reconnaissance
Presentationhost.exe	Execute
Print.exe	Alternate data streams Copy
Psr.exe	Reconnaissance
Rasautou.exe	Execute
Reg.exe	Alternate data streams
Regasm.exe	AWL bypass Execute
Regedit.exe	Alternate data streams
Regini.exe	Alternate data streams
Register-cimprovider.exe	Execute
Regsvcs.exe	Execute AWL bypass
Regsvr32.exe	AWL bypass Execute
Replace.exe	Copy Download
Rpcping.exe	Credentials
Rundll32.exe	Execute Alternate data streams
Runonce.exe	Execute
Runscripthelper.exe	Execute
Sc.exe	Alternate data streams
Schtasks.exe	Execute
Scriptrunner.exe	Execute
SyncAppvPublishingServer.exe	Execute
Ttdinject.exe	Execute
Tttracer.exe	Execute Dump
vbc.exe	Compile
Verclsid.exe	Execute

Program	Possible exploits
Wab.exe	Execute
Wmic.exe	Alternate data streams Execute
Wscript.exe	Alternate data streams
Wsreset.exe	UAC bypass
Xwizard.exe	Execute

OTHER MS BINARIES

Program	Possible exploits
AgentExecutor.exe	Execute
Appvlp.exe	Execute
Bginfo.exe	Execute AWL bypass
Cdb.exe	Execute
csi.exe	Execute
Devtoolslauncher.exe	Execute
dnx.exe	Execute
Dotnet.exe	AWL bypass Execute
Dxcap.exe	Execute
Excel.exe	Download
Mftrace.exe	Execute
Msdeploy.exe	Execute AWL bypass
msxsl.exe	Execute AWL bypass
ntdsutil.exe	Dump
Powerpnt.exe	Download
rcsi.exe	Execute AWL bypass
Sqldumper.exe	Dump
Sqlps.exe	Execute
SQLToolsPS.exe	Execute
Squirrel.exe	Download AWL bypass Execute

OTHER MS BINARIES (II)

te.exe	Execute
Tracker.exe	Execute AWL bypass
Update.exe	Download AWL bypass Execute
vsjitdebugger.exe	Execute
Winword.exe	Download
Wsl.exe	Execute Download

LIBRARIES

Program	Possible exploits
Advpack.dll	AWL bypass Execute
Comsvcs.dll	Dump
Ieadvpack.dll	AWL bypass Execute
Ieaframe.dll	Execute
Mshtml.dll	Execute
Pcwutl.dll	Execute
Setupapi.dll	AWL bypass Execute
Shdocvw.dll	Execute
Shell32.dll	Execute
Syssetup.dll	AWL bypass Execute
Url.dll	Execute
Zipfldr.dll	Execute