L-Soft international, Inc.

GDPRSCAN Installation and Operating Guide For Windows, Linux, and MacOS

This document sets forth the installation and operation procedures for the GDPRSCAN PowerShell script provided by L-Soft international, Inc., for use with its LISTSERV mailing list manager.

Information in this document is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. L-Soft international, Inc. does not endorse or approve the use of any of the product names or trademarks appearing in this document.

All of L-Soft's manuals are available at the following URL: **http://www.lsoft.com/manuals.html**

L-Soft invites comment on its manuals. Please feel free to send your comments by
e-mail to: MANUALS@LSOFT.COM

Last Revised 14 Aug 2020
GDPRSCAN.PS1 1.0e

GDPRSCAN Installation and Operating Guide

Table of Contents

Overview

The European Union's General Data Protection Regulation (GDPR) has been in effect since May 25, 2018. GDPR doesn't just affect enterprises in the EU, though; theoretically at least, any entity that stores personal information pertaining to an EU citizen – regardless of whether or not that entity does business in the EU – is also subject to its provisions regarding personal data storage. If you're not sure about the basics of GDPR, you might want to take a look at our 2017 newsletter article entitled "Ready for GDPR? Test Your Knowledge, Get The Facts."

GDPR requires, among other things, that a company must be able to provide on demand a report in a common machine-readable format (such as XML) which lists every instance of a customer's personal data held by that company. For LISTSERV, that can be a tricky prospect, because personal data may be held in list archives, in changelogs, and of course in subscription lists themselves.

In response, L-Soft developed a PowerShell script which, using either the LCMD.EXE or LCMDX.EXE command interfaces that ship with the Windows version of LISTSERV, can pull the relevant data using standard LISTSERV commands and methods, and produce an XML report containing the results. While the script itself is Windows-specific, by using the LCMDX.EXE option (which communicates directly with the server's TCPGUI port), it is possible to generate reports from any unix-based LISTSERV site as well, so long as the site has the LISTSERV web interface enabled.

The script also works under PowerShell Core 6.1 and later, making it possible to run the script from Linux and MacOS workstations by using the unix version of 'lcmdx'.

Downloading the script and associated files

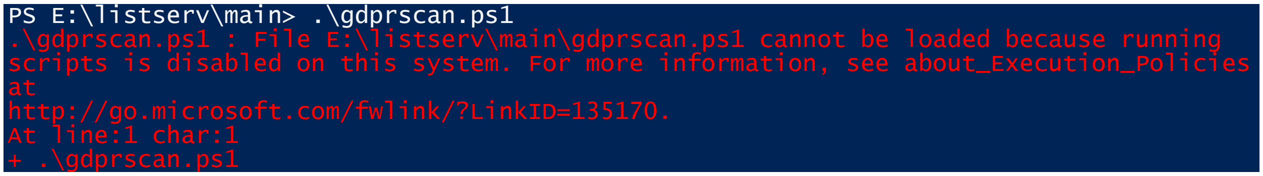
The script is available for download from http://download.lsoft.com/downloads/gdprscan/gdprscan.zip and comes bundled with copies of LCMD.EXE, LCMDX.EXE, and the source code for LCMDX (lcmdx.c) for users' convenience. (We don't provide an executable copy of lcmdx for Linux/MacOS, because it's usually best to compile and link the code locally against your existing libraries. We'll provide instructions for doing that below.)

Minimum PowerShell Version Required

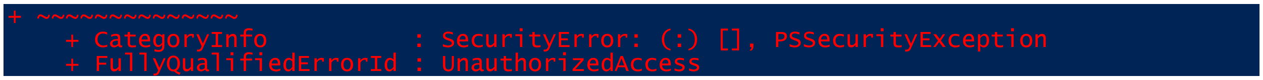
The GDPRSCAN requires at least PowerShell Version 3.0 on the machine from which it will be executed. PowerShell 5.x or greater is preferred.

PowerShell Execution Policy

Note that the Microsoft Windows version of PowerShell has a default execution policy of "Restricted", that is, PowerShell accepts only interactive commands and will not run scripts. Typically this results in an error something like the following:



```
PS E:\listserv\main> .\gdprscan.ps1
.\gdprscan.ps1 : File E:\listserv\main\gdprscan.ps1 cannot be loaded because running
scripts is disabled on this system. For more information, see about_Execution_Policies
at
http://go.microsoft.com/fwlink/?LinkID=135170.
At line:1 char:1
+ .\gdprscan.ps1
```



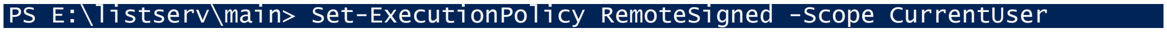
```
+ ~~~~~~~~~~~~~~~
    + CategoryInfo          : SecurityError: (:) [], PSSecurityException
    + FullyQualifiedErrorId : UnauthorizedAccess
```

In order to run the GDPRSCAN script, you must do one of two things:

- If you are running PowerShell from a standard Windows "run as administrator" command prompt, you can bypass the default execution policy by adding "-ExecutionPolicy Bypass" to the command, like this:

  ```
  E:\LISTSERV\MAIN>PowerShell -ExecutionPolicy Bypass -File .\gdprscan.ps1
  ```

- If you are running GDPRSCAN in a PowerShell console, you will need to elevate the execution policy level for the CurrentUser scope to at least "RemoteSigned". This can be done as follows:

  ```
  PS E:\listserv\main> Set-ExecutionPolicy RemoteSigned -Scope CurrentUser
  ```

  You will be prompted to ensure that this is really what you want to do.

Windows: Installing the script

Once you have downloaded the files, you can unpack them into any convenient directory, preferably one that is in your PATH. For instance, you may prefer to install them in a directory called C:\%USERPROFILE%\PROC, or even C:\PROC. If you are installing the files directly onto the LISTSERV machine, you may even unpack them into \LISTSERV\MAIN if you so choose. The most important point to observe is that LCMD.EXE and LCMDX.EXE must be available to the script, so they must be either placed in the same directory with the script or found somewhere in your PATH.

It is likely that you will have to unblock the script before PowerShell will allow it to be executed. This can be done in one of two ways:

- Open a PowerShell prompt, change to the directory where you have unpacked the files, and execute "Unblock-File gdprscan.ps1"; or
- Right-click the gdprscan.ps1 file in Windows Explorer, choose "Properties", click the "Unblock" button found at the bottom of the "General" tab

Windows: Named Pipes or TCPGUI?

You will need to decide whether GDPRSCAN will be using LCMD.EXE (which is a named-pipes interface) or LCMDX.EXE (which is a TCP/IP interface that talks to the TCPGUI port on the LISTSERV machine, in a similar manner to the way the WA interface works).

Note, however, that if you are using the script to pull GDPR reports from a unix LISTSERV site, you *must* use LCMDX.EXE, as the named-pipes interface used by LCMD.EXE is only useable with the Windows version of LISTSERV.

The interface is chosen by specifying an optional value for the -Method (minimum abbreviation: -m) parameter on the command line. Either

```
-Method LCMDX
```

or

```
-Method LCMD
```

can be used. The default is “LCMDX”.

Typically, the named-pipes interface will work only if the machine running the script is in the same Windows domain as the LISTSERV server machine, and you have not explicitly disabled named pipes on either your Windows client machine or the LISTSERV server machine, and so long as named pipe connections are not otherwise blocked from either end. You may also need to make a minor configuration change to LISTSERV, as by default, named-pipe requests are presumed to be coming from invoking_userid@NODE – for instance, john.doe@LISTSERV.EXAMPLE.COM. This may or may not be what you want. You can use LISTSERV's CMDPIPE_HOSTNAME= site configuration variable to change the hostname side of the address. For instance, if your enterprise addresses take the form of local_part@EXAMPLE.COM, you could set CMDPIPE_HOSTHAME=EXAMPLE.COM and restart LISTSERV to pick up the change.

The advantage to using named pipes is that the LISTSERV named pipes interface is secure and does not require password authentication. If password authentication is desired, or if you are using the script to run GDPR reports on a machine that is external to your local Windows domain, or is running on a unix machine, you will have to use the LCMDX.EXE TCPGUI interface instead.

Windows: Where to write the XML report?

By default, GDPRSCAN will write the resulting XML report to your Windows desktop. This may or may not be optimal for you, so there is an option to change it. If you wanted to change it to your "My Documents" directory, simply use the -XMLpath (minimum abbreviation: -x) to set it accordingly:

```
-XMLPath 'C:\Users\youruserid\My Documents'
```

Windows: Executing the script

Once you have installed the script and made any needed changes to the LISTSERV configuration, you will execute the script like this (optional command line arguments shown in square brackets []):

With LCMD (Named Pipes):

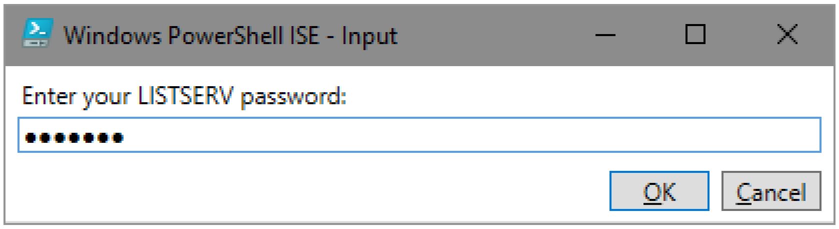
```
PS C:\PROC > .\gdprscan.ps1 -s listserv-hostname -t target-email [-d ALLlists | SYSTEM
| FULL]
```

With LCMDX (TCPGUI):

```
PS C:\PROC > .\gdprscan.ps1 -s listserv-hostname -t target-email -p postmaster-email
[-d ALLlists | SYSTEM | FULL]
```

When using the script with LCMDX, you will have to provide one additional piece of information to the script after running it – the LISTSERV personal password corresponding to the postmaster-email address you are using. The password is obtained securely (see the examples below) and is stored as a secure string while the program is running.

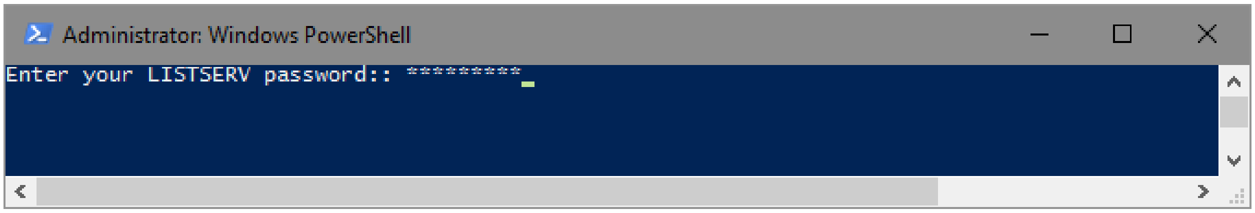
Example using the PowerShell ISE:



Enter your LISTSERV password:

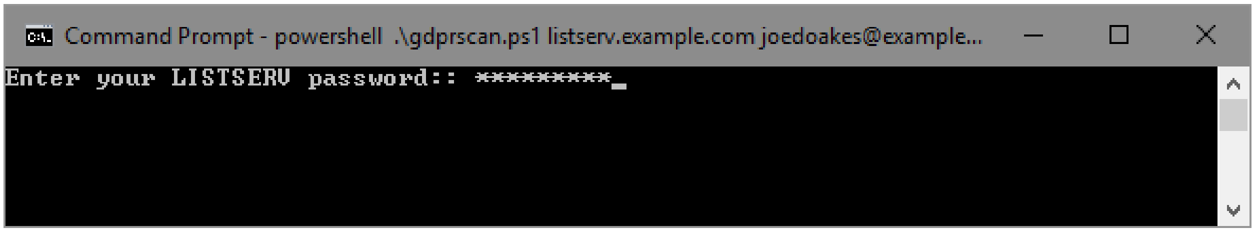
●●●●●●●

Example if executed from a PowerShell prompt (not the ISE):



```
Enter your LISTSERV password:: *********_
```

Example if executed from a Windows command prompt:


Command Prompt - powershell .\gdprscan.ps1 listserv.example.com joedoakes@example...

```
Enter your LISTSERV password:: *********_
```

The script will continue to execute after you hit <return>.

The final command line argument is optional, defining the depth of the changelog scan. For a normal (default) scan, this argument is not used. Changelog scanning levels are defined as follows:

Default (no argument)	Only the *listname*.changelog files for the lists to which the target email address is subscribed are scanned.
ALLlists	(minimum abbreviation: “ALL”) All *listname*.changelogs are scanned, regardless of whether the target email address is subscribed. (This may pick up information on lists to which the target email was subscribed in the past.)
SYSTEM	Same as the default, plus SYSTEM and NOLIST-* changelogs are scanned, if present.
FULL	All changelogs on the server are scanned.

If specified, these levels are mutually exclusive; only one may be specified per run.

The options are presented above in ascending order of how much time they will typically take to execute. On one L-Soft server, the ALL option resulted in a 51-minute-long scan for a single user;

however, significant network latency may have contributed to that test. Another L-Soft server with a very large SYSTEM.CHANGELOG processed the ALL option for a single user in 15 minutes.

Typically, scanning changelogs other than those belonging to the list(s) to which the target address is subscribed is an expensive operation, there may be little if any personal information for the target address found in them, and it may simply not be desirable to run that deep of a scan.

GDPR does not require data controllers to spend an unlimited amount of time on requests, and therefore, L-Soft has left the decision on depth of scan up to the customer.

Linux/MacOS: Installing the script

Installing the script on a Linux or MacOS machine presumes that you have already installed the latest version of Microsoft PowerShell Core, which at this writing is 6.1. Microsoft have published (and continue to update regularly) a useful article explaining how to go about doing that at this link.

You will also need to compile the lcmdx.c source code which is included in the gdprscan.zip bundle. This can be as simple as opening a terminal box and issuing the command

```
[root@linuxbox ~]# gcc -O lcmdx.c -o lcmdx
```

at the prompt. (Note that this also presumes that you have the 'gcc' compiler installed.)

If you are installing GDPRSCAN on a machine that is running LISTSERV, lcmdx may already be compiled; if not, check the $LSVROOT directory for lcmdx.c, and then simply run `make lcmdx' to compile and link the executable.

Once you have lcmdx compiled, you MUST copy it into /usr/local/bin or some other directory listed in your $PATH. You will also want to set appropriate ownership and permissions for lcmdx. For instance, `chmod 755 lcmdx; chown root:root lcmdx' will result in the following:

```
-rwxr-xr-x.  1 root      root 13384 Apr 11 10:42 lcmdx
```

which should allow any user to execute lcmdx. This may be more extreme than you prefer; the only constraint is that the ownership and permissions must be set so lcmdx can be executed by whomever needs to run gdprscan.

> NOTE: As stated, under Linux/MacOS, the script expects lcmdx to be installed in a common location which is included in the $PATH environment variable. One of the best places for that is /usr/local/bin , which is a "well-known" location for programs a normal user may run.
>
> Under Linux/MacOS, the script will not be able to find and execute lcmdx if it cannot be found in the $PATH.

Linux/MacOS: Where to write the XML report?

By default, GDPRSCAN will write the resulting XML report to your Windows desktop. This may or may not be optimal for you, so there is an option to change it. If you wanted to change it to your “Documents" directory, simply use the -XMLpath (minimum abbreviation: -x) to set it accordingly:

```
-XMLPath '/home/myuserid/Documents'
```

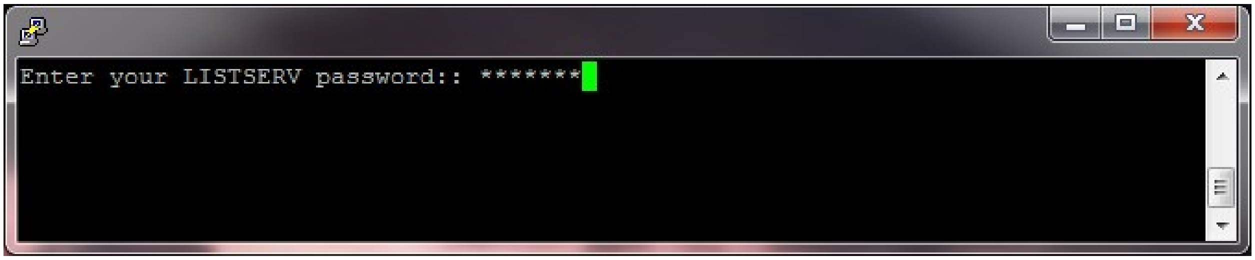
Linux/MacOS: Executing the script

Once you have installed the script, you will execute the script like this (optional command line arguments shown in square brackets []):

```
PS /home/you > ./gdprscan.ps1 -s listserv-hostname -t target-email -p postmaster-email
[-d ALLlists | SYSTEM | FULL]
```

You will have to provide one additional piece of information to the script after running it – the LISTSERV personal password corresponding to the postmaster-email address you are using. The password is obtained securely and is stored as a secure string while the program is running.

Example:



```
Enter your LISTSERV password:: *******
```

The script will continue to execute after you hit <return>.

The final command line argument is optional, defining the depth of the changelog scan. For a normal (default) scan, this argument is not used. Changelog scanning levels are defined as follows:

Default (no argument)	Only the *listname*.changelog files for the lists to which the target email address is subscribed are scanned.
ALLlists	(minimum abbreviation: “ALL”) All *listname*.changelogs are scanned, regardless of whether the target email address is subscribed. (This may pick up information on lists to which the target email was subscribed in the past.)
SYSTEM	Same as the default, plus SYSTEM and NOLIST-* changelogs are scanned, if present.
FULL	All changelogs on the server are scanned.

If specified, these levels are mutually exclusive; only one may be specified per run.

The options are presented above in ascending order of how much time they will typically take to execute. On one L-Soft server, the ALL option resulted in a 51-minute-long scan for a single user;

however, significant network latency may have contributed to that test. Another L-Soft server with a very large SYSTEM.CHANGELOG processed the ALL option for a single user in 15 minutes.

Typically, scanning changelogs other than those belonging to the list(s) to which the target address is subscribed is an expensive operation, there may be little if any personal information for the target address found in them, and it may simply not be desirable to run that deep of a scan.

GDPR does not require data controllers to spend an unlimited amount of time on requests, and therefore, L-Soft has left the decision on depth of scan up to the customer.

Command Line Parameter Reference

Command line parameters for GDPRSCAN are non-positional in nature. Each parameter requires an identifying flag. If no parameters are provided at run-time, certain basic assumptions are made, and you will be prompted for values for the parameters marked in the following table as “Mandatory”. A basic sample command line would be something like

```
.\gdprscan.ps1 -s listserv.example.com -t joe@example.com -p admin@example.com -v f
```

While the parameters are non-positional, specifying them in the order shown without the parameter flags also works. However, if the flags are *not* used, you MUST provide a non-blank, valid value for each parameter. The only exception is for the -Server parameter; the server name may be specified in the first position without a flag if the rest of the parameters used are specified with flags. For instance,

```
.\gdprscan.ps1 listserv.example.com -v f -p admin@example.com -t joe@example.com
```

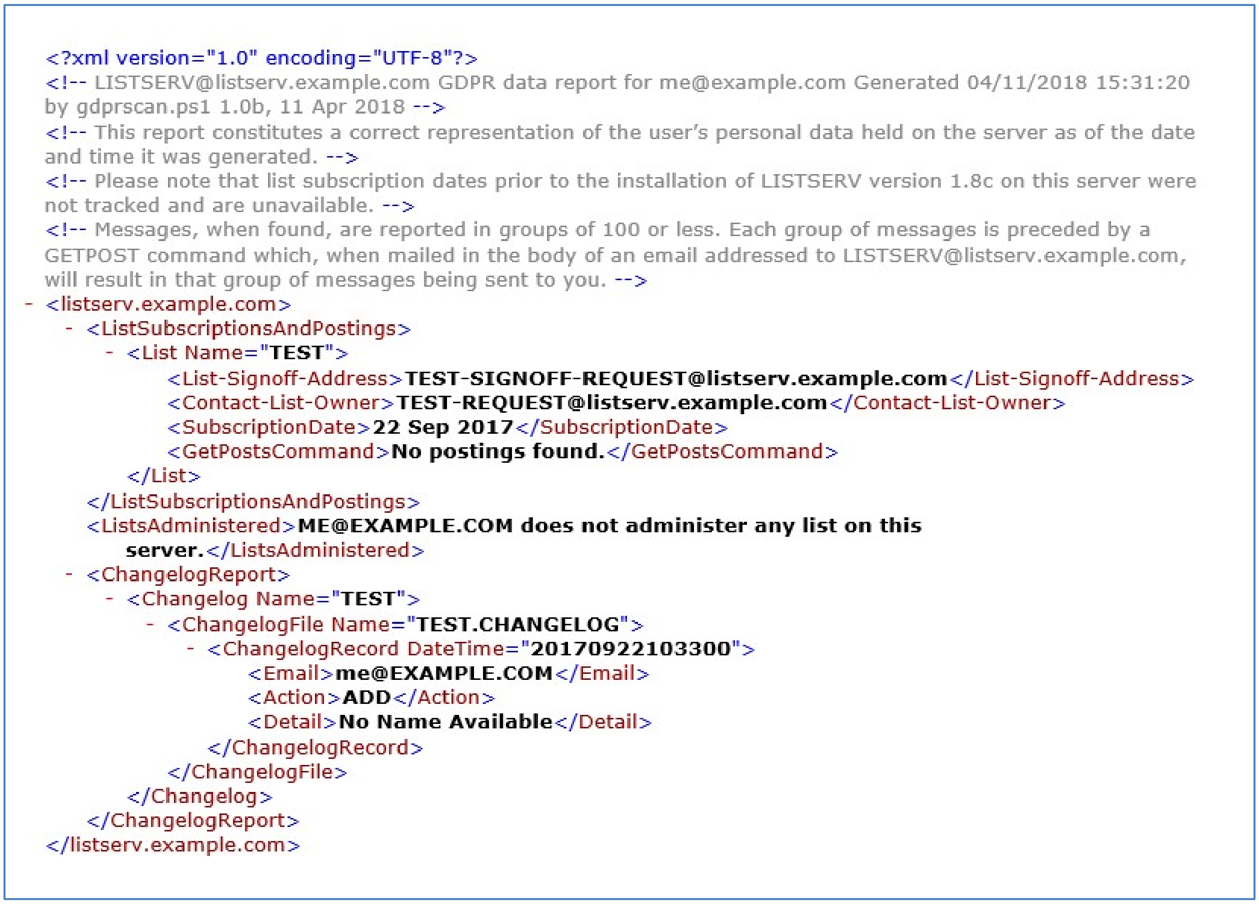
works, even though the parameters following the server hostname are specified “out of order.”

Parameter	Alias	Default	Description	Mandatory?
-Server	-s	none	For LCMDX, the fully-qualified domain name (FQDN) registered in DNS for the target LISTSERV server. For LCMD, the NETBIOS name of the LISTSERV machine. For LCMDX only: If the LISTSERV site configuration variable TCPGUI_PORT= has been configured to a value other than the default of 2306, you must also specify the port number here in the usual way, e.g., if you have set TCPGUI_PORT= 42306, then you must specify it thusly: `-s listserv.example.com:42306`	**YES**
-TargetEmail	-t	none	The email address to be searched.	**YES**
-PostmasterEmail	-p	none	The email address of the person running the report. Must be either a LISTSERV postmaster or a list owner. List owners	**YES**

			have access only to information pertaining to their own lists.	
-VerboseOutput	-v	True	Determines whether to echo the report information back to the console screen. As the reports can become extremely verbose, it may be preferred to disable verbose output by setting it to “False”. Setting this parameter to False will result in only very basic console output, sufficient to assure the operator that the report is running. “T” and “F” are acceptable values and are case-insensitive.	No
-ReportDepth	-d	none (basic changelog report)	One of “ALLlists”, “SYSTEM”, or “FULL”, depending on the depth of the changelog reporting desired. The default is to not specify a report depth, which results in a changelog report being run only on the list-level changelogs for the lists to which the target email is currently subscribed.	No
-Method	-m	LCMDX	Windows only. Either “LCMDX” (TCPGUI) or “LCMD” (named pipes). Windows users should see the section above entitled “Windows: Named Pipes or TCPGUI?” for more information. Linux and MacOS users will always use LCMDX and do not need to specify a value for this parameter.	No
-XMLPath	-x	none (Windows Desktop directory or Linux/MacOS current directory)	The path to the location of the resulting XML report. The default is to not specify a value, which results in the report being written to the Windows desktop directory or to the Linux/MacOS current directory. If specified, the path should be enclosed in single quotes.	No

Sample Output

A (very minimal) sample XML report generated with GDPRSCAN looks like this, when loaded into a browser:



```
  <?xml version="1.0" encoding="UTF-8"?>
  <!-- LISTSERV@listserv.example.com GDPR data report for me@example.com Generated 04/11/2018 15:31:20
  by gdprscan.ps1 1.0b, 11 Apr 2018 -->
  <!-- This report constitutes a correct representation of the user's personal data held on the server as of the date
  and time it was generated. -->
  <!-- Please note that list subscription dates prior to the installation of LISTSERV version 1.8c on this server were
  not tracked and are unavailable. -->
  <!-- Messages, when found, are reported in groups of 100 or less. Each group of messages is preceded by a
  GETPOST command which, when mailed in the body of an email addressed to LISTSERV@listserv.example.com,
  will result in that group of messages being sent to you. -->
- <listserv.example.com>
  - <ListSubscriptionsAndPostings>
    - <List Name="TEST">
        <List-Signoff-Address>TEST-SIGNOFF-REQUEST@listserv.example.com</List-Signoff-Address>
        <Contact-List-Owner>TEST-REQUEST@listserv.example.com</Contact-List-Owner>
        <SubscriptionDate>22 Sep 2017</SubscriptionDate>
        <GetPostsCommand>No postings found.</GetPostsCommand>
      </List>
    </ListSubscriptionsAndPostings>
    <ListsAdministered>ME@EXAMPLE.COM does not administer any list on this
      server.</ListsAdministered>
  - <ChangelogReport>
    - <Changelog Name="TEST">
      - <ChangelogFile Name="TEST.CHANGELOG">
        - <ChangelogRecord DateTime="20170922103300">
            <Email>me@EXAMPLE.COM</Email>
            <Action>ADD</Action>
            <Detail>No Name Available</Detail>
          </ChangelogRecord>
        </ChangelogFile>
      </Changelog>
    </ChangelogReport>
  </listserv.example.com>
```

What data is included in the LISTSERV GDPR report?

Reports generated by GDPRSCAN are a "best effort" attempt to create a report containing all references to the requesting user as of the time the report is run. The report attempts only to determine the following:

- A list of the lists on the server to which the target address is currently subscribed
- A list of all postings found in each subscribed list's archives (if the list has archives) which were originated by the target address, including the post number, date/time, subject, and a GETPOST command for each 100 postings found for retrieval of those posts
- A list of all lists on the server for which the target address is currently a list owner, a list editor, and/or a list moderator
- A list of all list-level changelogs on the server which contain references to the target address
- A list of registration data held by LISTSERV, which contains the target address and/or the registered full name associated with it, along with the originating IP address recorded for the user's last web interface login.
- (Optional) A list of all references found in the SYSTEM.CHANGELOG and any NOLIST-*.CHANGELOG files which exist on the server.

You will note that there is no attempt made to search for the requesting user's email address in archived message bodies, nor is there any attempt made to "fuzzy match" the email address to other possible addresses used by the requesting user. GDPRSCAN also does not attempt to search archives of lists to which the requesting user may have been subscribed in the past, although typically that information will be exposed in POST records found in the list-level changelog reports, if changelogs exist for those lists.

Each invocation of GDPRSCAN is intended to produce output only for a single email address. It would likely be possible to expand the script to cover other possibilities, but L-Soft believes that the script as it exists constitutes a reasonable search through LISTSERV data which does not potentially expose third-party personal information to the requestor.

Caveats and Disclaimers

This information should not be considered as legal advice, and compliance is the responsibility of each organization.

L-Soft strongly recommends that each report be analyzed for any inappropriate data prior to being sent on to the requestor. L-Soft does not guarantee or warrant that any random piece of changelog data or subject line text from messages will not contain third-party personal information. It is the sole responsibility of the person or organization generating the report to vet the report prior to sending it to the requestor.

Use of the GDRPSCAN script and the associated LCMD/LCMDX LISTSERV interfaces constitutes the user's agreement to hold L-Soft international, Inc. harmless for any accidental or purposeful exposure of personal information consequent to its use.

Prerequisites

- LISTSERV change-logging is NOT enabled by default. Change-logging MUST be enabled in LISTSERV in order to provide changelog reports. For information on how to set up the system-level changelog, see this link. For information on how to set up list-level changelogs, see this link.
- For Windows, a reasonably-recent version of PowerShell (5.x or later is preferred). For Linux or MacOS users, the latest version of PowerShell Core should be used.
- LISTSERV 16.5 or later, with a build date of 9 Apr 2018 or later, is required in order to run changelog reports. Earlier builds will produce a message in the XML stating that changelog reports cannot be run because the installed LISTSERV version does not support them.
- LISTSERV POSTMASTER-level access is required to run the comprehensive, server-level reports.
- List owners may use the script to run reports against lists they own. However, such a report may not fully meet the GDPR criteria if the target address is subscribed to lists on the server which are not owned by the script invoker.

Support

Customers with paid-up LISTSERV maintenance may obtain help and report problems with the script by emailing support@lsoft.com.

Other L-Soft GDPR resources

The EU General Data Protection Regulation (GDPR)

The EU General Data Protection Regulation (GDPR) FAQ

____