

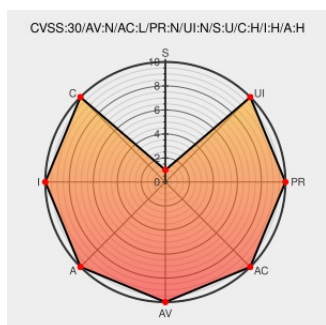


# CVE-2017-7938

Published on: 04/20/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:40 PM UTC

## CVE-2017-7938

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Dmitry Deepmagic Information Gathering Tool](#) from [Mor-pah.net](#) contain the following vulnerability:

Stack-based buffer overflow in DMitry (Deepmagic Information Gathering Tool) version 1.3a (Unix) allows attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a long argument. An example threat model is automated execution of DMitry with hostname strings found in local log files.

CVE-2017-7938 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.8 - CRITICAL**

Attack  
Vector

Attack  
Complexity

Privileges  
Required

User  
Interaction

**NETWORK**

**LOW**

**NONE**

**NONE**

Scope

Confidentiality  
Impact

Integrity  
Impact

Availability  
Impact

**UNCHANGED**

**HIGH**

**HIGH**

**HIGH**

CVSS2 Score: **7.5 - HIGH**

Access  
Vector

Access  
Complexity

Authentication

**NETWORK**

**LOW**

**NONE**

Confidentiality  
Impact

Integrity  
Impact

Availability  
Impact

**PARTIAL**

**PARTIAL**

**PARTIAL**

## CVE References

Description

Tags

Link

Dmitry 1.3a - Local Buffer Overflow

[www.exploit-db.com](#)  
[Proof of Concept](#)  
[text/html](#)

[EXPLOIT-DB 41898](#)

|                                                        |                                                                                                                                                                      |                                                                                                                                                                                          |
|--------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CXSecurity - IDS                                       | <a href="#">Exploit</a><br><a href="#">Third Party Advisory</a><br><a href="#">cxsecurity.com</a><br><a href="#">text/html</a>                                       |  <a href="#">MISC cxsecurity.com/issue/WLB-2017040113</a>                                                |
| Dmitry 1.3a Local Stack Buffer Overflow ≈ Packet Storm | <a href="#">Exploit</a><br><a href="#">Third Party Advisory</a><br><a href="#">VDB Entry</a><br><a href="#">packetstormsecurity.com</a><br><a href="#">text/html</a> |  <a href="#">MISC packetstormsecurity.com/files/142210/Dmitry-1.3a-Local-Stack-Buffer-Overflow.html</a> |

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to [comment@cve.report](mailto:comment@cve.report).

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

| Type                                                                              | Vendor                      | Product                                                     | Version | Update | Edition | Language |
|-----------------------------------------------------------------------------------|-----------------------------|-------------------------------------------------------------|---------|--------|---------|----------|
| Application                                                                       | <a href="#">Mor-pah.net</a> | <a href="#">Dmitry Deepmagic Information Gathering Tool</a> | 1.3a    | All    | All     | All      |
| Application                                                                       | <a href="#">Mor-pah.net</a> | <a href="#">Dmitry Deepmagic Information Gathering Tool</a> | 1.3a    | All    | All     | All      |
| cpe:2.3:a:mor-pah.net:dmitry_deepmagic_information_gathering_tool:1.3a:*:*:*:*:*: |                             |                                                             |         |        |         |          |
| cpe:2.3:a:mor-pah.net:dmitry_deepmagic_information_gathering_tool:1.3a:*:*:*:*:*: |                             |                                                             |         |        |         |          |

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)