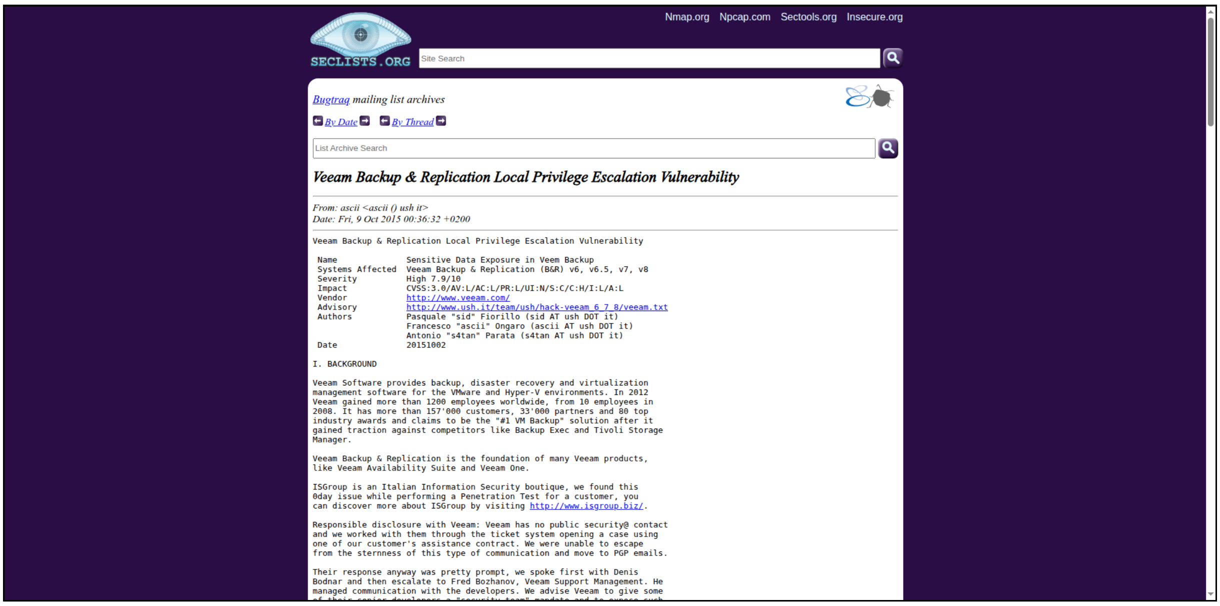
PRESS REVIEW ARCHIVE

Digital Media Monitoring & Documentation Service

Source URL:	https://seclists.org/bugtraq/2015/Oct/51
Archived Date:	August 15, 2025 at 15:13
Published:	February 05, 2023
Document Type:	Web Page Archive
Wayback Machine:	https://web.archive.org/web/*/https://seclists.org/bugtraq/2015/Oct/51

Page Screenshot



Bugtraq mailing list archives

Veeam Backup & Replication Local Privilege Escalation Vulnerability

From: ascii <ascii () ush it>
Date: Fri, 9 Oct 2015 00:36:32 +0200

```
Veeam Backup & Replication Local Privilege Escalation Vulnerability

 Name              Sensitive Data Exposure in Veem Backup
 Systems Affected  Veeam Backup & Replication (B&R) v6, v6.5, v7, v8
 Severity          High 7.9/10
 Impact            CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:L/A:L
 Vendor            http://www.veeam.com/
 Advisory          http://www.ush.it/team/ush/hack-veeam_6_7_8/veeam.txt
 Authors           Pasquale "sid" Fiorillo (sid AT ush DOT it)
                   Francesco "ascii" Ongaro (ascii AT ush DOT it)
                   Antonio "s4tan" Parata (s4tan AT ush DOT it)
 Date              20151002

I. BACKGROUND

Veeam Software provides backup, disaster recovery and virtualization
management software for the VMware and Hyper-V environments. In 2012
Veeam gained more than 1200 employees worldwide, from 10 employees in
2008. It has more than 157'000 customers, 33'000 partners and 80 top
industry awards and claims to be the "#1 VM Backup" solution after it
gained traction against competitors like Backup Exec and Tivoli Storage
Manager.

Veeam Backup & Replication is the foundation of many Veeam products,
like Veeam Availability Suite and Veeam One.

ISGroup is an Italian Information Security boutique, we found this
0day issue while performing a Penetration Test for a customer, you
can discover more about ISGroup by visiting http://www.isgroup.biz/.

Responsible disclosure with Veeam: Veeam has no public security@ contact
and we worked with them through the ticket system opening a case using
one of our customer's assistance contract. We were unable to escape
from the sternness of this type of communication and move to PGP emails.

Their response anyway was pretty prompt, we spoke first with Denis
Bodnar and then escalate to Fred Bozhanov, Veeam Support Management. He
managed communication with the developers. We advise Veeam to give some
```

Veeam Backup & Replication Local Privilege Escalation Vulnerability

From: ascii <ascii () ush it>
Date: Fri, 9 Oct 2015 00:36:32 +0200

Veeam Backup & Replication Local Privilege Escalation Vulnerability

Name	Sensitive Data Exposure in Veem Backup
Systems Affected	Veeam Backup & Replication (B&R) v6, v6.5, v7, v8
Severity	High 7.9/10
Impact	CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:L/A:L
Vendor	http://www.veeam.com/
Advisory	http://www.ush.it/team/ush/hack-veeam_6_7_8/veeam.txt
Authors	Pasquale "sid" Fiorillo (sid AT ush DOT it) Francesco "ascii" Ongaro (ascii AT ush DOT it) Antonio "s4tan" Parata (s4tan AT ush DOT it)
Date	20151002

I. BACKGROUND

Veeam Software provides backup, disaster recovery and virtualization management software for the VMware and Hyper-V environments. In 2012 Veeam gained more than 1200 employees worldwide, from 10 employees in 2008. It has more than 157'000 customers, 33'000 partners and 80 top industry awards and claims to be the "#1 VM Backup" solution after it gained traction against competitors like Backup Exec and Tivoli Storage Manager.

Veeam Backup & Replication is the foundation of many Veeam products, like Veeam Availability Suite and Veeam One.

ISGroup is an Italian Information Security boutique, we found this 0day issue while performing a Penetration Test for a customer, you can discover more about ISGroup by visiting http://www.isgroup.biz/.

Responsible disclosure with Veeam: Veeam has no public security@ contact and we worked with them through the ticket system opening a case using one of our customer's assistance contract. We were unable to escape from the sternness of this type of communication and move to PGP emails.

Their response anyway was pretty prompt, we spoke first with Denis Bodnar and then escalate to Fred Bozhanov, Veeam Support Management. He managed communication with the developers. We advise Veeam to give some of their senior developers a "security team" mandate and to expose such team to external, direct, communication. The people we spoke to did their best and were extremely kind but they must be supported by a corporate process.

Prior vulnerabilities in Veeam: It's very difficult to say if Veeam had previous vulnerabilities, there are no CVE assigned to this vendor both on Nist and to it's CPE (cpe:/:veeam). Information to customers of the vulnerability is shown in the "other" section of the changelog: "Removed weakly encrypted username and password logging from guest processing components using networkless (VIX) guest interaction mode. Veeam thanks Pasquale Fiorillo and Francesco Ongaro of ISGroup for vulnerability discovery.".

The latest version of the software at the time of writing can be obtained from:

http://www.veeam.com/kb2068
http://forums.veeam.com/veeam-backup-replication-f2/8-0-common-issues-and-fixes-t24157.html#p130849
http://www.veeam.com/vmware-esx-backup.html

II. DESCRIPTION

The vulnerability allows a local Windows user, even with low privileges as the ones provided to an anonymous IIS's virtualhost user, to access Veeam Backup logfiles that include a double-base64 encoded version of the password used by Veeam to run.

The affected component is VeeamVixProxy, created by default on installation and the user must be a privileged Local Administrator or a Domain Administrator.

For example the wizard for adding a VMware or Hyper-V Backup Proxy explicitly state "Type in an account with local administrator privileges on the server you are adding. Use DOMAIN\USER format for domain accounts, or HOST\USER for local accounts.".

We conservatively refer to this issue as a Local Administrator Privilege Escalation but the use of Domain Administrator accounts is not discouraged, if not advised, and we saw this pattern in our customerâ€™s production infrastructures.

TLDR: Anything able to read VeeamVixProxy logfiles, world readable by default, can escalate to Local or Domain Administrator.

III. ANALYSIS

Veeam Backup & Replication (B&R) v6, v6.5, v7, v8 store VeeamVixProxy logfiles in a directory accessible by Everyone and with permissions that make them readable by Everyone (Everyone is, in the Microsoft Windows terminology, the equivalent of the Unixâ€™s nobody user).

Such logs, that are continuously generated, contain a Local or Domain Administration user and password in an easily reversible (obfuscated) format.

In versions of Veeam prior to 8 a bug prevented log rotation [3,4], on older systems there could be a large amount of logs and thus an extensive history of past and current Local or Domain Administrator credentials.

A) Logfiles readable by Everyone

As shown in http://www.veeam.com/kb1789 the default log path is

```
  Windows Server 2003: %allusersprofile%\Application Data\Veeam\Backup
  Windows Server 2008 and up: %programdata%\Veeam\Backup
```

Our evidence is for Windows Server 2003, access to the needed files are guaranteed to the Windows group "Everyone" so any local user, even the ones used to map IIS sites, can access them.

This pose all the information contained in the logfiles at risk and is a violation of the principle of least privilege.

https://en.wikipedia.org/wiki/Principle_of_least_privilege

B) Double encoded password in Logfiles

The install/execution username and password is stored double-base64 encoded in Veeam Backup "VeeamVixProxy" logfiles.

Such files exists in "Veeam\Backup" with a name scheme as follows:

```
VeeamVixProxy_%dd%mm%yyyy.log
```

```
eg: VeeamVixProxy_16072015.log
```

The password is present in multiple points of the log-file and the files are generated contentiously.

In this scenario, a Local File Read vulnerability could lead to full system compromise given the fact that an attacker can re-use such credentials by RDP or RPC (eg: psexec).

The log format leaking the credentials is:

```
<date> <time> <number> Blob Data: <base64>
```

```
eg: 01/07/2015 1.33.42 3936 Blob Data:
IwAAAAoAAABWAGUAZQBhAG0AVQBzAGUAcgAQAAAAVQAyAFYAagBjAG0AVgAwAA
```

The "<base64>" of interest has the following format:

```
  echo 'IwAAAAoAAABWAGUAZQBhAG0AVQBzAGUAcgAQAAAAVQAyAFYAagBjAG0AVgAwAA'\
  | base64 -d | hexdump -C
  00000000  23 00 00 00 0a 00 00 00  56 00 65 00 65 00 61 00
|#.......V.e.e.a.|
  00000010  6d 00 55 00 73 00 65 00  72 00 10 00 00 00 55 00
|m.U.s.e.r.....U.|
  00000020  32 00 56 00 6a 00 63 00  6d 00 56 00 30 00
|2.V.j.c.m.V.0.  |
```

First byte is \x23 (#), followed by a NULL and a newline (\x0a), followed by a NULL. Next bytes specify the username, followed by a DLE (data link escape) and a NULL. Everything in the first base64 container is in UTF16.

```
echo -n "isgroup" | iconv -t UTF-16LE | hexdump -C
```

What follows is the most interesting part, a base64 representation of the password.

```
echo -en "U2VjcmV0" | base64 -d
Secret
```

Since the VeeamVixProxy files are continuously written the leak will occur even if administrators delete them. An official fix from Veeam is needed in order to fully resolve the vulnerability.

This vulnerability is especially dangerous when the "VeeamAdmin" (or whenever you called it) is also a Domain Administration user.

IV. WORKAROUND

Update: on 8 October 2015 Veeam B&R 8.0 Update 3 has been released and the vendor states it fixes the vulnerability. You are strongly advised to update to the latest version. We did not investigate but will update you on ush.it if needed.

Follow this steps to mitigate the issue meanwhile an official patch is released:

If you are on Windows 2003 environment fix the permission on "%alluserprofile%\Application Data\Veeam\Backup" path so that only "Administrators" group can read it.

If you are on Windows 2008 environment fix the permission on "%programdata%\Veeam\Backup\" so that only "Administrators" group can read it.

Create a scheduled task to delete this logfiles from disk.

VI. VENDOR RESPONSE

Vendor released Update 3 of Veeam B&R 8.0 that contains the proper security patch. At the time of this writing an official patch is currently available.

VII. CVE INFORMATION

Mitre assigned the CVE-2015-5742 for this vulnerability, internally to Veeam it's referred as Case #00984117.

VIII. DISCLOSURE TIMELINE

20150723 Bug discovered
20150724 Vulnerability disclosed to ISGroup's Partners
20150805 Request for CVE to Mitre
20150805 Got CVE-2015-5742 from cve-assign (fast!)
20150806 Details disclosure to Support/Denis Bodnar and CVE
20150806 Escalation to Fred Bozhanov (fast!) will fix in Veeam B&R v8
20150818 Veeam closes the ticket
20150923 ISGroup asks for updates, no release date from vendor
20150923 We extend the disclosure date as 30 Sept will not be met
20151008 Veeam releases Update 3 for Version 8.0
20151008 Advisory disclosed to the public

IX. REFERENCES

[1] Top 10 2013-A6-Sensitive Data Exposure
https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure

[2] Access Control Cheat Sheet
https://www.owasp.org/index.php/Access_Control_Cheat_Sheet

[3] http://forums.veeam.com/veeam-backup-replication-f2/veeamvixproxy-log-t20579.html
User reporting 5.5 GB of VeeamVixProxy_date.log files

[4] http://forums.veeam.com/veeam-backup-replication-f2/feature-request-t28404.html
User reporting 7 GB of VeeamVixProxy logs on 7.0.0.839

[4] http://www.veeam.com/kb1825
How to Change the settings related to Veeam Backup &

    Replication Log Files

[5] http://www.veeam.com/kb1789
    How to locate and collect VSS/VIX log files from Guest OS

Want to access this document in HTML?

http://www.ush.it/2015/10/08/veeam-backup-replication-6-7-8-local-privilege-escalation-vulnerability/

X. CREDIT

Pasquale "sid" Fiorillo, Francesco "ascii" Ongaro and Antonio "s4tan"
Parata are credited with the discovery of this vulnerability.

Pasquale "sid" Fiorillo
web site: http://www.ush.it/
mail: sid AT ush DOT it

Francesco "ascii" Ongaro
web site: http://www.ush.it/
mail: ascii AT ush DOT it

Antonio "s4tan" Parata
web site: http://www.ush.it/
mail: s4tan AT ush DOT it

XI. LEGAL NOTICES

Disclaimer: The information in the advisory is believed to be accurate
at the time of publishing based on currently available information. Use
of the information constitutes acceptance for use in an AS IS condition.
There are no warranties with regard to this information. Neither the
author nor the publisher accepts any liability for any direct, indirect,
or consequential loss or damage arising from use of, or reliance on,
this information.

By Date By Thread

Current thread:

Veeam Backup & Replication Local Privilege Escalation Vulnerability ascii (Oct 09)

Site Search

Nmap Security Scanner

Ref Guide
Install Guide
Docs
Download
Nmap OEM

Npcap packet capture

User's Guide
API docs
Download
Npcap OEM

Security Lists

Nmap Announce
Nmap Dev
Full Disclosure
Open Source Security
BreachExchange

Security Tools

Vuln scanners
Password audit
Web scanners
Wireless
Exploitation

About

About/Contact
Privacy
Advertising
Nmap Public Source License