PRESS REVIEW ARCHIVE

Digital Media Monitoring & Documentation Service

Source URL: https://securityaffairs.com/40891/hacking/veeam-zero-day.html

Archived Date: August 15, 2025 at 15:00

Published: October 09, 2015

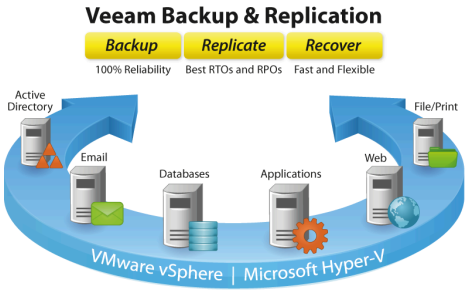
Document Type: Web Page Archive

Wayback Machine: https://web.archive.org/web/*/https://securityaffairs.com/40891/hacking/veeam-zero-day.html

Page Screenshot

TIME TO UPDATE YOUR VEEAM TO FIX A VEEAMVIXPROXY VULNERABILITY

Pierluigi Paganini October 09, 2015



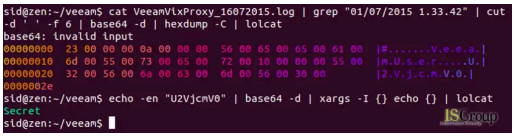
The vulnerability allows a local unprivileged user of a Windows guest to gain Local and/or Domain Administrator access when VeeamVixProxy is active, the de-facto default in VMWare and Hyper-V environments.

Pasquale `sid` Fiorillo, Francesco `ascii` Ongaro from ISGroup, an Italian Security firm, and Antonio `s4tan` Parata from ush team, have just released a critical security advisory for any version of Veeam Backup & Replication prior to 8 Update 3 (released today, October 8th, 2015).

Veeam Software provides backup, disaster recovery and virtualizationmanagement software for the VMware and Hyper-V environments. The ISGroup team has discovered this 0day in the Veeam Software while performing a Penetration Test for a customer.

"The vulnerability allows a local unprivileged user of a Windows guest to gain Local and/or Domain Administrator access when VeeamVixProxy is active, the de-facto default in VMWare and Hyper-V environments." states the advisory.

The issue potentially involves 157,000 customers and 9.1 million Virtual Machines worldwide and could lead to full Domain Administrator compromise of the affected infrastructures.



This vulnerability is caused by a component, VeeamVixProxy, that logs in an obfuscated way the administrator username and password used by Veeam to run.

An attacker could easily "decode" the password in cleartext. From subsequent analysis, it turns out that Veeam's admin user is often a Domain Administrator user and this enables a scenario in which an unprivileged user, or even a hacked IIS website, inside a single Virtual Machine, can escalate his privileges to Domain Administrator.

Even if Domain escalation is not possible, the attacker will at least get the Local Administrator's credentials.

Users are strongly advised to update their systems to the latest version released by the vendor.

About the Author Francesco Ongaro

Senior Security Researcher at ISGroup

Edited by Pierluigi Paganini

(Security Affairs – Veeam Backup & Replication , hacking)

Hacking | Pierluigi Paganini | Security Affairs | Veeam | VeeamVixProxy | virtual machine. | zero-Day

YOU MIGHT ALSO LIKE

Pierluigi Paganini August 15, 2025

Cisco fixed maximum-severity security flaw in Secure Firewall Management Center

Read more

Pierluigi Paganini August 15, 2025

'Blue Locker' Ransomware Targeting Oil & Gas Sector in Pakistan

Read more

LEAVE A COMMENT

Name

Email

Comments

LEAVE COMMENT

NEWSLETTER

Subscribe to my email list and stay up-to-date!

Your email address

SIGN UP

RECENT ARTICLES

Cisco fixed maximum-severity security flaw in Secure Firewall Management Center

SECURITY / August 15, 2025

'Blue Locker' Ransomware Targeting Oil & Gas Sector in Pakistan

MALWARE / August 15, 2025

Hackers exploit Microsoft flaw to breach Canada 's House of Commons

HACKING / August 15, 2025

Norway confirms dam intrusion by Pro-Russian hackers

HACKTIVISM / August 14, 2025

Zoom patches critical Windows flaw allowing privilege escalation

SECURITY / August 14, 2025

securityaffairs

To contact me write an email to:

Pierluigi Paganini :
pierluigi.paganini@securityaffairs.co

LEARN MORE

QUICK LINKS