The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
www.cisa.gov/tlp
Information may be distributed without restriction, subject to standard copyright rules.

DATE(S) ISSUED:
03/14/2022

SUBJECT:
Multiple Vulnerabilities in Veeam Backup & Replication Could Allow for Remote Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Veeam Backup & Replication that could allow for remote code execution. Veeam Backup & Replication is a backup solutions for virtual environments. Successful exploitation of the most severe of these vulnerabilities could allow for remote code execution within the context of the application. Depending on the privileges associated with this application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

THREAT INTELLIGENCE:
There are no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:

- Veeam Backup & Replication version 9.5, 10, 11

RISK:
Government:

- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in Veeam Backup & Replication that could allow for remote code execution. Details of the vulnerabilities are as follows:

- A vulnerability exists in which an unauthenticated user can access internal API functions over port 9380/TCP (CVE-2022-26500).
- A vulnerability exists in which the above vulnerability may be used to allows executing malicious code remotely without authentication (CVE-2022-26501)
- A vulnerability exists in Veeam.Backup.PSManager.exe in which authentication using non-administrative domain credentials is allowed when Veeam Backup & Replication is installed with a registered Microsoft System Center Virtual Machine Manager (SCVMM) server (CVE-2022-26504)

Successful exploitation of the most severe of these vulnerabilities could allow for remote code execution within the context of the application. Depending on the privileges associated with this application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. If this application has been configured to have fewer user rights on the system, exploitation of this vulnerability could have less impact than if it was configured with administrative rights.

RECOMMENDATIONS:
We recommend the following actions be taken:

- Install the updates provided by Veeam immediately after appropriate testing
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.

Apply the Principle of Least Privilege to all systems and services.

REFERENCES:
CVE:
https://learn.cisecurity.org/e/799323/vename-cgi-name-CVE-2022-26500/rsfny/273021816?h=3wrtWHmPvXfIbD5mSrz7JUL7bbGGRcknGzThXTBQlNw
https://learn.cisecurity.org/e/799323/vename-cgi-name-CVE-2022-26501/rsfp1/273021816?h=3wrtWHmPvXfIbD5mSrz7JUL7bbGGRcknGzThXTBQlNw
https://learn.cisecurity.org/e/799323/vename-cgi-name-CVE-2022-26504/rsfp3/273021816?h=3wrtWHmPvXfIbD5mSrz7JUL7bbGGRcknGzThXTBQlNw

Veeam:
https://www.veeam.com/kb4288
https://www.veeam.com/kb4290