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

https://www.cisa.gov/tlp

Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

DATE(S) ISSUED:

05/04/2021

SUBJECT:

A Vulnerability in HPE Edgeline Infrastructure Manager Software Could Allow for Remote Code Execution

OVERVIEW:

A vulnerability has been discovered in HPE Edgeline Infrastructure Manager Software that could allow for remote code execution. HPE Edgeline Infrastructure Manager Software was made to aggregate the management of Edgeline ComputeDevices. It is delivered as a Virtual Machine image (OVA) targeted at running on VMware ESXi, workstation,or player. Edgeline Infrastructure Manager supports discovery, monitoring, and management of EdgelineConverged Edge Systems.

Successful exploitation of this vulnerability could result in remote code execution within the context of the application, an attacker gaining the same privileges as the logged-on user, or the bypassing of security restrictions. Depending on the permission associated with the application running the exploit, an attacker could then install programs; view, change, or delete data.

THREAT INTELLIGENCE:

There are currently no reports of this vulnerability being exploited in the wild.

SYSTEMS AFFECTED:

- HPE Edgeline Infrastructure Management Software - Prior to version 1.22

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:

A vulnerability has been discovered in HPE Edgeline Infrastructure Manager Software. The vulnerability could be remotely exploited to bypass remote authentication leading to execution of remote commands, gaining privileged access, causing denial of service, and changing the

configuration. Specifically this vulnerability is due to an issue related to how HPE handles password resets for administrator accounts. Successful exploitation of this vulnerability could result in remote code execution within the context of the application, an attacker gaining the same privileges as the logged-on user, or the bypassing of security restrictions. Depending on the permission associated with the application running the exploit, an attacker could then install programs; view, change, or delete data.

RECOMMENDATIONS:
The following actions should be taken:

- Apply the appropriate patch provided by HPE (HPE Edgeline Infrastructure Manager version 1.22 or later).
- Run all software as a nonprivileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to download, accept or execute files from untrusted and unknown sources.
- Remind users not to visit untrusted websites or follow links provided by untrusted or unknown sources.
- Evaluate read, write, and execute permissions on all newly installed software.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:
CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-29203

HP:
https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbgn04124en_us
https://support.hpe.com/hpesc/public/docDisplay?docId=a00066458en_us&docLocale=en_US

ThreatPost:
https://threatpost.com/hewlett-packard-critical-bug-edge/165797/