HPE Edgeline Infrastructure Manager Unauthenticated Information Disclosure

Medium

← View More Research Advisories

Synopsis

Tenable has found an information disclosure vulnerability in HPE Infrastructure Manager (EIM). HPE EIM allows an unauthenticated remote attacker to download a compressed support debugging dump file:

```
curl -sk --tlsv1.2 https://<eim-host>/eim/v1/supportdump  | gunzip > /tmp/supportdump.log
```

The decompressed support dump file is the concatenation of contents from many log files intended to be looked at by the vendor support team for troubleshooting. The start of the support dump file contains text:

> Note: This output contains potentially sensitive configuration about your EIM installation. Protect its content as you would your systems themselves.

So the dump file can contain sensitive information.

Solution

See vendor advisory.

Additional References

https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbgn04180en_us

Disclosure Timeline

05/07/2021 - Vulnerability discovered
05/17/2021 - Tenable discloses to vendor
05/18/2021 - HPE acknowledges report.
06/17/2021 - Tenable requests status update. HPE states fix is in progress.
07/19/2021 - Tenable requests status update.
07/20/2021 - HPE states that a fix is in progress.
08/06/2021 - HPE informed Tenable that a fix is available.

Risk Information

CVE ID: CVE-2021-26586
Tenable Advisory ID: TRA-2021-33
CVSSv3 Base / Temporal Score: 5.3 / 5.0
CVSSv3 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
Affected Products: HPE Edgeline Infrastructure Management Software - Prior to 1.24
Risk Factor: Medium

Advisory Timeline

August 9, 2021 - Initial release.

Nessus

→ View all Products

FEATURED SOLUTIONS

Application Security

Building Management Systems

Cloud Security Posture Management

Compliance

Exposure Management

Finance

Healthcare

IT/OT

Ransomware

State / Local / Education

US Federal

Vulnerability Management

Zero Trust

→ View all Solutions

CUSTOMER RESOURCES

Resource Library

Community & Support

Customer Education

Tenable Research

Documentation

Trust and Assurance

Nessus Resource Center

Cyber Exposure Fundamentals

System Status

CONNECTIONS

Blog

Contact Us

Careers

Investors

Events

Media