GE Digital Product Security Communication

Title:	GE Digital APM Classic Vulnerabilities
Vulnerability ID:	GED 20 - 04
CVE:	CVE-2020-16240; ICSA-20-266-01 GE Digital APM Classic
Communication Release Date:	September 22, 2020

Summary

Three vulnerabilities (Vulnerabilities) were reported to GE Digital by Accenture having the potential to impact the Affected Software. After assessing the Vulnerabilities, GE Digital determined they could be exploited to compromise the password security, server-side authorization and Direct Object Reference (IDOR) features of the Affected Software, permitting an unauthorized user without admin privileges to access information and modify user data in the Affected Software. GE believes exploitation of the Vulnerabilities is only possible if an attacker was first authenticated.

As of this Communications Release Date, GE Digital believes it addressed the Vulnerabilities through its most updated release of APM Classic v 4.5, released September 18, 2020.

Users are advised to upgrade the Affected Software immediately, in accordance with the Solution below.

Affected Software

GE Digital APM Classic product v4.4.x and earlier

Solution

GE Digital recommends users upgrade all instances of the Affected Software to GE Digital's APM Classic product v. 4.5 immediately, released September 18, 2020 (Upgrade).

The Upgrade contains what GE believes are mitigation measures to help ensure the Vulnerabilities cannot be exploited.

To obtain the latest versions of the Update please contact your local GE Digital representative at https://digitalsupport.ge.com/communities/CC_Contact

Other Recommendations

GE Digital believes the Upgrade is the most effective way to address the Vulnerabilities. Workarounds may mitigate some of the issues but only the Upgrade will fully address the identified Vulnerabilities.

For those customers electing not to implement the Upgrade, GE Digital strongly recommends such customers conduct frequent audits of the Affected Software, in addition to carefully monitoring unprivileged users' activity, in addition to taking other measures to assist with securing the affected endpoints.

GE Digital thanks the cyber security researchers at Accenture for bringing information about the Vulnerabilities to GE Digital's attention.

Disclaimers

This Communication is subject to terms and conditions contained in customers' underlying license agreements or other applicable agreements. Due to ongoing product enhancements, GE Digital reserves the right to change or update its advisories without advance notification. GE DIGITAL DISCLAIMS ANY REPRESENTATION OR WARRANTY THAT ITS PRODUCTS WILL OPERATE FREE FROM ERROR, INTERRUPTION, OR DISRUPTION, INCLUDING, WITHOUT LIMITATION, DUE TO CYBER-ATTACKS, MALICIOUS OR OTHERWISE, OR FROM INTERRUPTIONS, OR THAT ANY SOLUTION PROVIDED BY GE WILL PROVIDE COMPLETE OR COMPREHENSIVE PROTECTION AGAINST ALL POSSIBLE SECURITY VULNERABILITIES OR UNAUTHORIZED INTRUSIONS, INCLUDING WITH RESPECT TO THE VULNERABILITY.

Auto-Notification

Please visit the customer profile page on the support site to sign up for auto-notifications for GE Digital products to receive immediate notice of security alerts and information.

Instructions on "How to sign up for Auto-Notifications for updates" can be found here; https://digitalsupport.ge.com/communities/en_US/Article/How-to-sign-up-for-SIM-Auto-Notification-for-GE-Intelligent-Platforms-software-products-KB12680-en-US

Change Log

Date	Change(s)
September 22, 2020	Initial release