Produkt-Sicherheitshinweis

GE VERNOVA

Smallworld SWMFS – Unsachgemäße Authentifizierung

CVE-2025-3222

GE Vernova Electrification Software SWMFS – Sicherheitslücke aufgrund unsachgemäßer Authentifizierung

Sicherheitslücke-ID: CVE-2025-3222
CVSS v4.0-Bewertung:9,3
CVSS-Schweregrad: Kritisch
CVSS v4.0-Vektor: CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

Kommunikationsdatum: 08.10.2025

Übersicht

Der Geschäftsbereich Electrification Software von GE Vernova (GE Vernova) hat Kenntnis von einer Schwachstelle erhalten, die sich auf den Authentifizierungsmechanismus (Schwachstelle) seiner Smallworld Master File Server (SWMFS) (betroffene Software) in Smallworld-Bereitstellungen von Version 3.0.0 bis 5.3.3 (für Linux-Bereitstellungen) und Version 5.3.4 (für Windows-Bereitstellungen) beeinträchtigen und zu unbeabsichtigtem Verhalten führen könnte.

Nach der Bewertung der Sicherheitslücken für die betroffene Software kam GE Vernova zu dem Schluss, dass die Sicherheitslücke ausgenutzt werden könnte, um die Authentifizierung zu umgehen und möglicherweise erweiterte Befehle auszuführen.

Die Ausnutzung der Sicherheitslücke ist nur für Benutzer möglich, die über Kenntnisse des Systems, des zugrunde liegenden Protokolls und der Rechte verfügen, die mit Benutzern mit bereits bereitgestelltem Zugriff verbunden sind. Eine sichere Bereitstellung und eine strenge Zugriffsverwaltung für Benutzer sind unerlässlich. GE Vernova empfiehlt seinen Kunden dringend, die neuesten Anweisungen des Secure Deployment Guide (SDG) – Smallworld Documentation zu befolgen.

GE Vernova hat das Problem in Smallworld v5.3.4 für Linux-SWMFS-Benutzer und v5.3.5 für Windows-SWMFS-Benutzer behoben.

Diese Empfehlung wird im Rahmen einer Vereinbarung zur koordinierten Offenlegung bereitgestellt und ist ausschließlich für die internen Sicherheitsmaßnahmen und Abhilfemaßnahmen der Empfängerorganisation bestimmt. Die hierin enthaltenen Informationen sind vertraulich und dürfen bis zum koordinierten Veröffentlichungsdatum (6.11.2025**) nicht weitergegeben, zitiert oder öffentlich bekannt gegeben werden. Eine unbefugte Offenlegung kann gegen Vertraulichkeitsverpflichtungen verstoßen und die Sicherheit der Kunden gefährden.

Aufgrund der vielen strengen Anforderungen an Betriebstechnologie (OT) und industrielle Steuerungssysteme (ICS) empfiehlt GE Vernova aktuellen Benutzern dringend, ihre umfassenden Verteidigungsstrategien, einschließlich Netzwerksegmentierung, zu überprüfen, um das tatsächliche Risiko dieser Schwachstelle in ihrer Umgebung zu verstehen. Zur Unterstützung dieses Prozesses wurde ein Open-Source-Modell entwickelt, das hier zu finden ist: Industrial Vulnerability Scoring System (IVSS).

Betroffene Software

Betroffen

Alle Smallworld-Implementierungen (SW), die keine Desktop-Authentifizierung über einen Authentifizierungsserver wie UAA oder Zitadel verwenden und die sicheren Implementierungsrichtlinien nicht befolgen. Dies war ab SW5.3.4 für Bereitstellungen verfügbar, die Linux zum Ausführen von SWMFS verwenden, und ab SW5.3.5 für Bereitstellungen, die Windows zum Ausführen von SWMFS verwenden. Daher können Produkte von SW3.0.0 bis SW5.3.3 nicht so konfiguriert werden, dass die CVE entfernt wird.

Nicht betroffen

- Alle Smallworld-Bereitstellungen, die die Desktop-Authentifizierung über einen Authentifizierungsserver verwenden und die Richtlinien für die sichere Bereitstellung befolgen.

Lösung

GE Vernova empfiehlt Benutzern, entsprechend ihrem Anwendungsfall und ihrer Architektur ein Upgrade auf die oben aufgeführte, nicht betroffene Version durchzuführen, da dies die umfassendste Methode zur Behebung der Sicherheitslücke ist.

Außerdem wird Benutzern dringend empfohlen, die SDG-Anweisungen zu befolgen. Die vollständigen SDG finden Sie in der Smallworld-Dokumentation.

Um die neueste Version von SWMFS zu erhalten, wenden Sie sich bitte an Ihren lokalen Support-Mitarbeiter im Customer Center.

GE Vernova dankt Théo GOBINET und Azaël MARTIN vom ENGIE IT Offensive Cybersecurity Team dafür, dass sie das Unternehmen auf die Sicherheitslücke aufmerksam gemacht haben.

Haftungsausschluss

Die in dieser Mitteilung enthaltene CVE-Kennung hat zum Zeitpunkt dieser Mitteilung den Status „RESERVED" (reserviert). Sie wird zur Information der Kunden weitergegeben und nach koordinierter Offenlegung und Veröffentlichung der Mitteilung in der CVE-Datenbank öffentlich zugänglich gemacht.

Diese Empfehlung (Empfehlung) unterliegt den Bedingungen Ihrer zugrunde liegenden Lizenzvereinbarungen oder anderen geltenden Vereinbarungen mit GE Vernova. Aufgrund laufender Produktverbesserungen behält sich GE VERNOVA das Recht vor, seine Empfehlungen (einschließlich dieser Empfehlung) ohne vorherige Benachrichtigung zu ändern oder zu aktualisieren. GE VERNOVA DIGITAL LEHNT JEGLICHE ZUSICHERUNG ODER GEWÄHRLEISTUNG AB, DASS SEINE PRODUKTE, DIENSTLEISTUNGEN ODER LÖSUNGEN FEHLERFREI, UNTERBRECHUNGSFREI ODER STÖRUNGSFREI FUNKTIONIEREN, EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF CYBER-ANGRIFFE, böswilligen oder sonstigen Cyberangriffen, oder dass die von GE VERNOVA angebotenen Produkte, Dienstleistungen oder Lösungen einen vollständigen oder umfassenden Schutz vor allen möglichen Sicherheitslücken oder unbefugten Zugriffen bieten, einschließlich der Sicherheitslücke.

Automatische Benachrichtigung

Bitte besuchen Sie die Kundenprofilseite auf der Support-Website, um sich für automatische Benachrichtigungen für GE Vernova Software-Produkte anzumelden und sofortige Benachrichtigungen zu Sicherheitswarnungen und Informationen zu erhalten.

Anweisungen finden Sie hier: So melden Sie sich für automatische Benachrichtigungen an.

Änderungsprotokoll

Datum	Änderung(en)
7.10.2025	**Erstversion**

Diese Empfehlung wird im Rahmen einer Vereinbarung zur koordinierten Offenlegung bereitgestellt und ist ausschließlich für die internen Sicherheitsmaßnahmen und Abhilfemaßnahmen der Empfängerorganisation bestimmt. Die hierin enthaltenen Informationen sind vertraulich und dürfen bis zum koordinierten Veröffentlichungsdatum (6.11.2025**) nicht weitergegeben, zitiert oder öffentlich bekannt gegeben werden. Eine unbefugte Offenlegung kann gegen Vertraulichkeitsverpflichtungen verstoßen und die Sicherheit der Kunden gefährden.

Diese Empfehlung wird im Rahmen einer Vereinbarung zur koordinierten Offenlegung bereitgestellt und ist ausschließlich für die internen Sicherheitsmaßnahmen und Abhilfemaßnahmen der Empfängerorganisation bestimmt. Die hierin enthaltenen Informationen sind vertraulich und dürfen bis zum koordinierten Veröffentlichungsdatum (6.11.2025**) nicht weitergegeben, zitiert oder öffentlich bekannt gegeben werden. Eine unbefugte Offenlegung kann gegen Vertraulichkeitsverpflichtungen verstoßen und die Sicherheit der Kunden gefährden.