Produkt-Sicherheitshinweis

GE VERNOVA

Smallworld SWMFS Beliebige Dateioperationen

CVE-2025-7719

GE Vernova Electrification Software SWMFS Arbitrary File Ops

Sicherheitslücke ID: CVE-2025-7719
CVSS v4.0-Bewertung:5,3
CVSS-Schweregrad: Mittel
CVSS v4.0-Vektor: CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N

Kommunikationsdatum: 08.10.2025

Übersicht

Der Geschäftsbereich Electrification Software von GE Vernova (GE Vernova) hat Kenntnis von einer Sicherheitslücke erhalten, die es einem Benutzer ermöglichen könnte, Dateien (Sicherheitslücke) auf dem System, auf dem die Smallworld Master File Server (SWMFS)-Software (betroffene Software) gehostet wird, willkürlich zu manipulieren. Dies betrifft alle Smallworld-Implementierungen vor Version 5.3.6.

Nach der Bewertung der Sicherheitslücke für die betroffene Software kam GE Vernova zu dem Schluss, dass die Sicherheitslücke ausgenutzt werden könnte, um wichtige Dateien auf dem Server abzurufen, zu ändern, zu speichern oder zu löschen, was zu unbeabsichtigten Folgen führen könnte.

Die Ausnutzung der Sicherheitslücke ist nur für Benutzer mit Kenntnissen des Systems möglich. Eine sichere Bereitstellung und eine strenge Zugriffsverwaltung für Benutzer sind unerlässlich. GE Vernova empfiehlt Kunden dringend, die neuesten Anweisungen des Secure Deployment Guide (SDG) – Smallworld Documentation zu befolgen.

GE Vernova hat das Problem in SWMFS v5.36.6 behoben, das in Core Spatial Technology v5.3.6 veröffentlicht wurde.

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

- SWMFS v5.35.0 und früher

Lösung

GE Vernova empfiehlt Anwendern, 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 vollständige 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 Ankündigung zu ändern oder zu

aktualisieren. GE VERNOVA DIGITAL LEHNT JEGLICHE ZUSICHERUNG ODER GEWÄHRLEISTUNG AB, DASS SEINE PRODUKTE, DIENSTLEISTUNGEN ODER LÖSUNGEN FREI VON FEHLERN, UNTERBRECHUNGEN ODER STÖRUNGEN SIND, 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.

Eine Anleitung 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.