Product Security Bulletin

Evolving Product Security for Evolving Threats

Default SQL Credentials Leading to Remote Code Execution

Product Overview

- Product Impacted: All versions of NeuroWorks and SleepWorks software.
- Product Use: Used for the acquisition, display, archive, review and analysis of EEG and PSG physiological signals.
- Product Use Environment: These software solutions are typically found in private practice or hospital rooms near a patient's bedside or in neurology and sleep treatment areas.

Summary

- This product security bulletin DOC-065601 revision 01 was created August 9, 2023.
- As part of responsible disclosure practices, a security configuration documentation flaw in "DOC-007279: XLSecurity Site Administrator Reference" stating Natus does not recommend changing default passwords for local Microsoft SQL Server accounts was reported to Natus as "Default Password for Natus NeuroWorks EEG Software MSSQL Database", CWE: CWE-1393.
- The report of this finding was acknowledged by Natus Product Security on June 26, 2023.
- As a result, Natus corrected the documentation flaw and released revision G of the "DOC-007279: XLSecurity Site Administrator Reference" on July 21, 2023.
- Revision G of "DOC-007279: XLSecurity Site Administrator Reference" now states that Natus recommends changing default passwords for local Microsoft SQL Server accounts using the Credential Cache functionality introduced in NeuroWorks and SleepWorks version 8.4 GMA3.
- This documentation flaw affects both versions of NeuroWorks and SleepWorks supported at the time of the report, version 9 and version 8. Older unsupported versions do not have the Credential Cache functionality.

For More Information

- Natus customers can contact Natus Technical Service to obtain the most recent version of "DOC-007279: XLSecurity Site Administrator Reference" as needed.

- The updated “DOC-007279: XLSecurity Site Administrator Reference” document will be included in future releases of the software installation package for NeuroWorks/SleepWorks version 9.3, and the first general market availability release of version 10 (GMA2).

Additional Background

- John M. Jackson of Trustwave SpiderLabs discovered this vulnerability. Trustwave SpiderLabs then engaged Natus, via our established Coordinated Vulnerability Disclosure process.
- Trustwave SpiderLabs published recommendations state that NeuroWorks should release an official patch that allows backwards compatibility for integrated security (Windows authentication) for connecting to SQL databases. Natus agrees this would be the best mitigation and will work towards implementing MSSQL Windows authentication integration Neuroworks 10 currently under development. Natus is also investigating the feasibility of implementing MSSQL Windows authentication integration in a future patch release of Neuroworks version 9.
- Natus believes the current compensating control of using the Neuroworks Credential Cache functionality as a central tool to manage the credentials of MSSQL accounts reduces the risk associated with Default SQL Credentials Leading to Remote Code Execution to an acceptable level.
- Additionally, Natus will continue to follow established coordinated disclosure processes for any significant security vulnerabilities associated with our products or any updates associated with these vulnerabilities.
- At Natus, we take cybersecurity seriously and have teams actively engaged in these matters. We monitor our products and systems to assess any impacts associated with cybersecurity issues and take appropriate action, as needed.