SHARING SINCE 2010

H-ISAC®

HEALTH - ISAC

INFORMATIONAL

Joint Cybersecurity Information Sheet - Keeping PowerShell: Security Measures to Use and Embrace

TLP:WHITE

Jun 23, 2022

On June 22, 2022, a Cybersecurity Information Sheet was released by cybersecurity authorities from the United States, New Zealand, and the United Kingdom recommending proper configuration and monitoring of PowerShell, as opposed to removing or disabling PowerShell entirely. This will provide benefits from the security capabilities PowerShell can enable while reducing the likelihood of malicious actors using it undetected after gaining access to victim networks. The following recommendations will help defenders detect and prevent abuse by malicious cyber actors while enabling legitimate use by administrators and defenders.

This Cybersecurity Information Sheet from the National Security Agency (NSA), the Cybersecurity and Infrastructure Security Agency (CISA), the New Zealand National Cyber Security Centre (NZ NCSC), and the United Kingdom

National Cyber Security Centre (NCSC-UK) provides details on using PowerShell® and its security measures.

Health-ISAC recommends reading the attached Cybersecurity Information Sheet which can also be found here within Health-ISACs Threat Intelligence Portal (HTIP) Document Library for additional best practices concerning PowerShell.

Analysis

PowerShell® is a scripting language and command line tool included with Microsoft Windows®. Like Bash for open-source operating systems, PowerShell extends the user experience as an interface into the operating system. PowerShell was introduced in Windows Vista® and has evolved with each Windows version. PowerShell can help defenders manage the Windows operating system, by:

- Enabling forensics efforts
- Improving incident response
- Allowing automation of common or repetitive tasks

In Microsoft's cloud platform Azure®, PowerShell can help to manage Azure resources, permitting administrators and defenders to build automated tools and security measures. However, the extensibility, ease of use, and availability of PowerShell also present an opportunity for malicious cyber actors. Many publicly acknowledged cyber intrusions, including those by ransomware actors, have used PowerShell as a post-exploitation tool. This technique is not new, as malicious actors often find ways to target or use legitimate system software.

The authors' recommendations mitigate cyber threats without obstructing PowerShell's functionality, which aligns with Microsoft's guidance on maintaining operational PowerShell use. Blocking PowerShell hinders defensive capabilities that current versions of PowerShell can provide and prevents components of the Windows operating system from running properly. Recent versions of PowerShell with improved capabilities and options can assist defenders in countering abuse of PowerShell. The Australian Cyber Security Centre (ACSC) has also offered comprehensive configuration guidance on securing PowerShell.

Sources

Keeping PowerShell: Measures to Use and Embrace
Joint Cybersecurity Information Sheet

Reference(s)	Defense, CISA
Report Source(s)	CISA, NCSC, NSA

Release Date
Jun 22, 2022

Alert ID 9aac8bf9

This Alert has 1 attachment(s). To view or download the attachment(s), click "View Alert" to login to the web portal.

View Alert

Tags NSA, NCSC, CISA, PowerShell

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Share Threat Intel For guidance on sharing indicators with Health-ISAC via CSAP, please visit the Knowledge Base article CSAP “Share Threat Intel” Documentation at the link address provided here: https://health-isac.cyware.com/webapp/user/knowledge-base Additionally, this collaborative medium provides opportunities for attributed or anonymous sharing across ISACs and other cybersecurity related entities.

Turn off Categories For guidance on disabling this alert category, please visit the Knowledge Base article CSAP "Alert Categories" Toggle Documentation at the link address provided here: https://health-isac.cyware.com/webapp/user/knowledge-base

NCSC The National Cyber Security Centre (NCSC) is an organisation of the United Kingdom Government that provides advice and support for the public and private sector in how to avoid computer security threats. Based in London, it became operational in October 2016, and its parent organisation is GCHQ.

CISA CISA is the Nation’s risk advisor, working with partners to defend against today’s threats and collaborating to build more secure and resilient infrastructure for the future.

Access the Health-ISAC Intelligence Portal Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Cyware.

For Questions or Comments Please email us at toc@h-isac.org

Download Health-ISAC’s Information Sharing App.

For more update and alerts, visit: **https://health-isac.cyware.com**

If you are not supposed to receive this email,
please contact us at **toc@h-isac.org**.