

**TLP: WHITE**



## OSSI Cyber Threat Intelligence Program Product for the Healthcare and Public Health Sector

OSSI CTIP RFI 20160603-1: Zero Day Vulnerability

Date: 06/03/2016

**DISCLAIMER:** This product is provided “as is” for informational purposes only. The Department of Health and Human Services (HHS) does not provide any warranties of any kind regarding any information contained within. The HHS does not endorse any commercial product or service referenced in this product or otherwise. Further dissemination of this product is governed by the Traffic Light Protocol (TLP) marking in the header.

Dear HPH Sector Colleagues,

Hackers claim to have unearthed a zero-day vulnerability giving attackers admin rights to any Windows machine from Windows 2000 to a fully patched version of Windows 10. The zero day is for sale on the black market for \$90,000.

Can you provide any and all additional information in regards to this subject matter?

Below are the Open Source links:

<http://betanews.com/2016/06/01/windows-zero-day-exploit/>

<http://bgr.com/2016/06/01/windows-zero-day-exploit-sale/>

<https://threatpost.com/windows-zero-day-selling-for-90000/118380/>

The Cyber Threat Intelligence Program (CTIP) was established within the Department of Health and Human Services, Office of Security and Strategic Information (OSSI), in 2014. The OSSI CTIP monitors and analyzes all-source intelligence on cyber threats to the Healthcare and Public Health sector; provides timely, actionable cyber threat information; and solicits feedback and information requirements from the sector.

Please take a moment to let us know:

- Does this product provide information that is not available to you elsewhere?
- Is the information provided actionable?
- Is the level of context appropriate?

Please direct any comments or questions to [CTIP@hhs.gov](mailto:CTIP@hhs.gov) or 202-870-1864

**TLP: WHITE**