GLESEC INCIDENT REPORT

TLP-AMBAR

Organization	Inspira Health Network
Date	06/07/2018
Service	MSS-VM
Severity Level	Critical
Impact Level	Critical
Vulnerability Level	Critical

INCIDENT DESCRIPTION

Our Operations Center found and inconclusive response for a critical vulnerability on host 170.75.33.108, we encourage Inspira Health Network to check if this host counts with the MS15-034 (KB 3042553) security update already installed, if it is not installed, this host is at risk to have this vulnerability exploited.

This vulnerability affects Windows Server Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 and Windows Server 2008 R2 for x64-based Systems Service Pack 1

Microsoft identifies this as: “Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553)” and was published on “Microsoft Security bulletin MS15-034 – Critical”. CVE-2015-1635.

An attacker who successfully exploited this vulnerability could execute arbitrary code in the context of the System account by sending a specially crafted HTTP request to the affected system.

CONFIDENTIAL

GLESEC INCIDENT REPORT

TLP-AMBAR

RECOMMENDED ACTIONS

Apply Windows Security update MS15-034 (KB 3042553) The update addresses the vulnerability by modifying how the Windows HTTP stack handles requests.

COMMENTS AND RECOMMENDATIONS

By applying the security update mentioned in the Actions Taken section of this document this particular vulnerability is mitigated.

CONFIDENTIAL

GLESEC INCIDENT REPORT

TLP-AMBAR

GLESEC INFORMATION SHARING PROTOCOL

GLESEC CYBER SECURITY INCIDENTE REPORTS are in compliance with the U.S. Department of Homeland Security (DHS) Traffic-Light Protocol (TLP): TLP-White (Disclosure is Not Limited), TLP-Green (Limited Disclosure, Restricted Only to the Community), TLP-Amber (Limited Disclosure, Restricted to the Participant's Organization), and TLP-Red (Not for Disclosure, Restricted/ Classified - Only Shared with US DHS).

CONFIDENTIAL