GLESEC INCIDENT REPORT

TLP-AMBER

Organization	INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS (IEEE)
Date	7/2/18
Service	MSS-VM
Severity Level	Critical
Impact Level	Critical
Vulnerability Level	Critical

INCIDENT DESCRIPTION

Our Global Operations Center has found several critical vulnerabilities in a number of your hosts. The vulnerabilities are related to the detection of several unsupported versions of software in your systems.

As an overview, the vulnerabilities can be classified in the following categories:

- 14 Detection of Microsoft IIS 6.0, unsupported version.
- 12 Unsupported version of PHP detected, v5.4 or lower.
- 1 Multiple Vulnerabilities in Oracle GlassFish Server 3.1.2x

Detection of Microsoft IIS 6.0, unsupported version.

Microsoft ended support for Windows Server 2003 in June 15, 2015. This version of Windows Server includes IIS 6.0. This means that Microsoft no longer will develop security updates or patch for vulnerabilities present in this version of IIS, leaving the system as a perfect target for malicious attacks and could compromise your network. Currently there are several well documented vulnerabilities in this version of IIS that allow remote code execution (CVE-2009-3023), DoS (CVE-2009-2521) and Memory Overflow (CVE-2017-7269). We detected the following systems with IIS 6.0:

- 140.98.194.160
- 140.98.194.161
- 140.98.194.165
- 140.98.194.177 (training.comsoc.org)
- 140.98.194.192
- 140.98.194.202 (chapter.comsoc.org)
- 140.98.194.203 (e-new.comsoc.org)
- 140.98.194.52
- 140.98.194.56
- 140.98.194.62

GLESEC INCIDENT REPORT

TLP-AMBER

Unsupported version of PHP detected, v5.4 or lower.

PHP ended support for the version 5.4 in September 3, 2015. No new security patches will be developed for this version of PHP, this leaves the affected systems as prime targets for malicious attacks that could compromise your network. The vulnerabilities affecting the unsupported version of PHP allow remote code execution (CVE-2012-2386), bypass security measures (CVE-2018-10545) and can cause DoS (CVE-2015-8876). The following systems were detected with unsupported versions of PHP:

- 140.98.200.12 (eps.ieee.org)
- 140.98.200.30 (rs.ieee.org)
- 140.98.200.102 (taveqa2.ieee.org)
- 140.98.200.103 (taveqa3.ieee.org)
- 140.98.200.17 (pspb.ieee.org)

Multiple Vulnerabilities in Oracle GlassFish Server 3.1.2x

The reported version of Oracle GlassFish Server is prior to 3.1.2.15 and its affected by multiple vulnerabilities, for example: an information disclosure vulnerability that could allow a remote attacker obtain memory contents (CVE-2015-3237) and a remote code execution flaw (CVE-2016-3607).
The following system is affected by this vulnerability:

- 140.98.196.190

RECOMMENDED ACTIONS

For the IIS and PHP vulnerabilities, Microsoft and PHP encourage to update the software to the latest versions in order to obtain security patches to mitigate flaws and vulnerabilities in the software.

For Oracle GlassFish, in July 2016, Oracle released an Oracle Critical Patch Update and recommended to upgrade the GlassFish Servers to version 3.1.2.15 or later.

COMMENTS AND RECOMMENDATIONS

Since the vulnerabilities are present in systems that can be reached from the Internet, it is recommended to upgrade the systems to the latest versions as soon as possible. A malicious attacker could successfully infiltrate the network exploiting any of the vulnerabilities that are present in the hosts, compromising sensitive data.

In the event the exposed servers are used for research or testing purposes, GLESEC recommends to limit the access to those servers to the authorized parties only and filter other incoming connections to minimize the attack surface.

GLESEC INCIDENT REPORT

TLP-AMBER

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).

USA | PANAMA | ARGENTINA | MEXICO | COLOMBIA | PERU | CHILE | ECUADOR
Tel: +1 (609)-651-4246 / +(507)-836-5355