GDPR Assessment

Internal Vulnerability Scan Detail by Issue

Scan Date: 1/18/2018

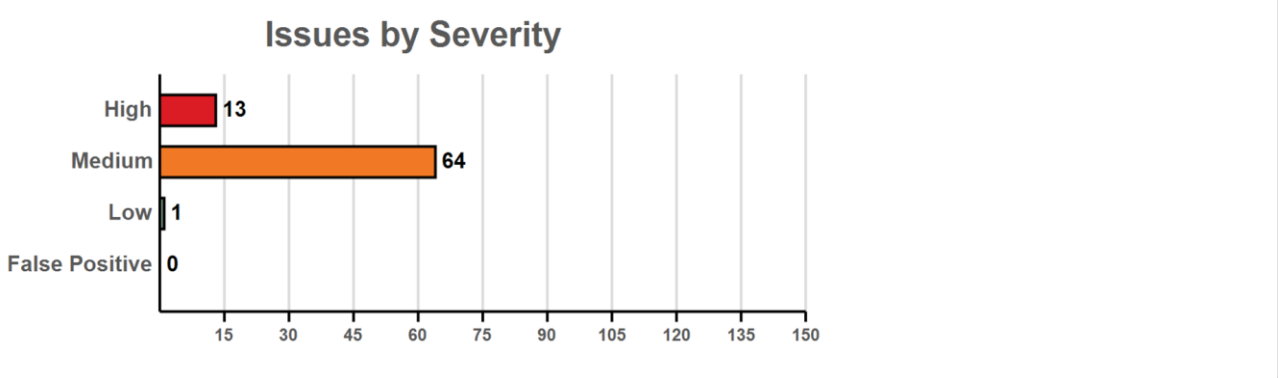
Prepared for:
Your Company
Prepared by:
Wem Technology Ltd

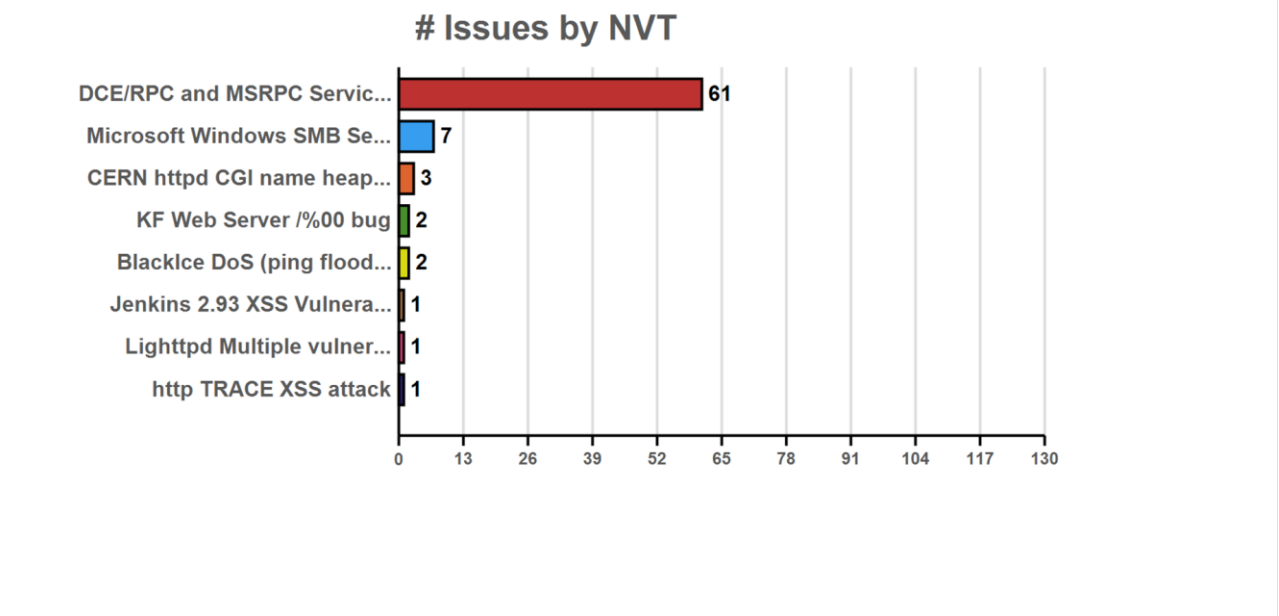
18/01/2018

Table of Contents

1 - Summary

This report gives details on hosts that were tested and issues that were found during the Internal Vulnerability Scan. The findings are grouped by category.

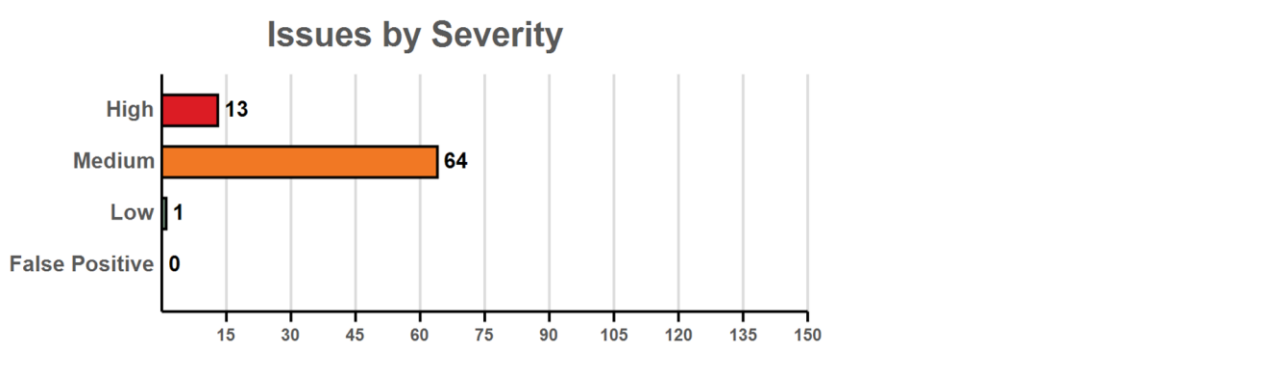




Issue	Count
DCE/RPC and MSRPC Services Enumeration Reporting	61
Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)	7
CERN httpd CGI name heap overflow	3
KF Web Server /%00 bug	2
BlackIce DoS (ping flood)	2
Jenkins 2.93 XSS Vulnerability (Windows)	1
Lighttpd Multiple vulnerabilities	1
http TRACE XSS attack	1

2 - Scan Details

This section details the issues discovered in order of severity. For each issue, the affected nodes are also listed.



2.1 - Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)

H	**High**: (CVSS: 9.3) **OID:** 1.3.6.1.4.1.25623.1.0.810676	445/tcp (microsoft-ds)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS17-010.

Affected Nodes
10.0.8.27, 10.0.8.39, 10.0.8.37, 10.0.8.70, 10.0.8.102, 10.0.8.104, 10.0.9.41

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to gain the ability to execute code on the target server, also could lead to information disclosure from the server. Impact Level: System

Solution
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/library/security/MS17-010

Vulnerability Insight
Multiple flaws exist due to the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests.

Vulnerability Detection Method
Send the crafted SMB transaction request with fid = 0 and check the response to confirm the vulnerability.
Details: Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389) (OID: 1.3.6.1.4.1.25623.1.0.810676) Version used: $Revision: 7543 $

References
https://support.microsoft.com/en-in/kb/4013078, https://technet.microsoft.com/library/security/MS17-010, https://github.com/rapid7/metasploit-framework/pull/8167/files

2.2 - Lighttpd Multiple vulnerabilities

H	**High**: (CVSS: 7.5) **OID:** 1.3.6.1.4.1.25623.1.0.802072	80/tcp (http)

Summary
This host is running Lighttpd and is prone to multiple vulnerabilities

Affected Nodes

10.0.8.169

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to execute arbitrary SQL commands and remote attackers to read arbitrary files via hostname. Impact Level: System/Application

Solution
Upgrade to 1.4.35 or higher, For updates refer to http://www.lighttpd.net/download

Vulnerability Insight
- mod_mysql_vhost module not properly sanitizing user supplied input passed via the hostname. - mod_evhost and mod_simple_vhost modules not properly sanitizing user supplied input via the hostname.

Vulnerability Detection Method
Send a crafted HTTP GET request and check whether it responds with error message. Details: Lighttpd Multiple vulnerabilities (OID: 1.3.6.1.4.1.25623.1.0.802072) Version used: $Revision: 7577 $

References
http://seclists.org/oss-sec/2014/q1/561, http://download.lighttpd.net/lighttpd/security/lighttpd_sa_2014_01.txt

2.3 - BlackIce DoS (ping flood)

Summary
It was possible to crash the remote machine by flooding it with 10 KB ping packets.

Affected Nodes
10.0.8.2, 10.0.9.199

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
A cracker may use this attack to make this host crash continuously, preventing you from working properly.

Solution
Upgrade your BlackIce software or remove it.

Vulnerability Detection Method
Details: BlackIce DoS (ping flood) (OID: 1.3.6.1.4.1.25623.1.0.10927) Version used: $Revision: 6315 $

2.4 - CERN httpd CGI name heap overflow

Summary
It was possible to kill the remote web server by requesting GET /cgi-bin/A.AAAA[...]A HTTP/1.0 This is known to trigger a heap overflow in some servers like CERN HTTPD.

Affected Nodes
10.0.8.1, 10.0.8.9, 10.0.8.4

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
A cracker may use this flaw to disrupt your server. It *might* also be exploitable to run malicious code on the machine.

Solution
Ask your vendor for a patch or move to another server

Vulnerability Detection Method

Details: CERN httpd CGI name heap overflow (OID: 1.3.6.1.4.1.25623.1.0.17231) Version used: $Revision: 6693 $

2.5 - http TRACE XSS attack

M	**Medium**: (CVSS: 5.8) **OID:** 1.3.6.1.4.1.25623.1.0.11213	80/tcp (http)

Summary
Debugging functions are enabled on the remote HTTP server. The remote webserver supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections. It has been shown that servers supporting this method are subject to cross-site-scripting attacks, dubbed XST for Cross-Site-Tracing, when used in conjunction with various weaknesses in browsers. An attacker may use this flaw to trick your legitimate web users to give him their credentials.

Affected Nodes
10.0.8.12

Vulnerability Detection Result
Solution: Add the following lines for each virtual host in your configuration file : RewriteEngine on RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK) RewriteRule .* - [F] See also http://httpd.apache.org/docs/current/de/mod/core.html#traceenable

Solution
Disable these methods.

Vulnerability Detection Method
Details: http TRACE XSS attack (OID: 1.3.6.1.4.1.25623.1.0.11213) Version used: $Revision: 6063 $

References
http://www.kb.cert.org/vuls/id/867593

2.6 - KF Web Server /%00 bug

M	**Medium**: (CVSS: 5.1) **OID:** 1.3.6.1.4.1.25623.1.0.11166	4444/tcp

Summary
Requesting a URL with '/%00' appended to it makes some versions of KF Web Server to dump the listing of the directory, thus showing potentially sensitive files.

Affected Nodes
10.0.8.2, 10.0.9.199

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
upgrade to the latest version of KF Web Server

Vulnerability Detection Method
Details: KF Web Server /%00 bug (OID: 1.3.6.1.4.1.25623.1.0.11166) Version used: $Revision: 8023 $

2.7 - DCE/RPC and MSRPC Services Enumeration Reporting

M	**Medium**: (CVSS: 5) **OID:** 1.3.6.1.4.1.25623.1.0.10736	135/tcp (loc-srv)

Summary
Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) or MSRPC services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.

Affected Nodes
10.0.1.9(DC), 10.0.1.4, 10.0.1.5(VPNGW9), 10.0.1.6(ISA1), 10.0.1.15(UTIL12), 10.0.1.16(DEVNFS), 10.0.1.21(RGATEWAY), 10.0.1.23, 10.0.1.41(FILE2012-1), 10.0.1.69(STORE01), 10.0.1.81(FINANCE), 10.0.1.100(HV00), 10.0.1.104(HV44), 10.0.1.120(HV42), 10.0.1.121(HV02), 10.0.8.0(MWEST-PC),

10.0.8.1(REX), 10.0.8.4(CCSVR01), 10.0.8.12(SVRTEST1), 10.0.8.14, 10.0.8.20(SVRDEV3), 10.0.8.33(CONFERENCEROOM), 10.0.8.35(BROWND), 10.0.8.40(PSIMPSON-PC), 10.0.8.41(QA-PC), 10.0.8.44(JD-WIN7), 10.0.8.47(PKWIN8), 10.0.8.53(PSIMPSON-WIN7TEST), 10.0.8.55(CONFROOM), 10.0.8.67(DEVTFSBUILD), 10.0.8.69(ISA1), 10.0.8.76(SVRDEMO1), 10.0.8.80(PS01), 10.0.8.86(SVRRFT1), 10.0.8.88(JRAWIN8K1QA3), 10.0.8.96(MWEST-WIN864), 10.0.8.97(RANR), 10.0.8.103(USER-HP), 10.0.8.106(P-HOME), 10.0.8.107(VPNGW), 10.0.8.109(SVRTEST2), 10.0.8.133(WRKMARCUS-PC), 10.0.9.18(PSIMPSON-WIN764), 10.0.9.44(JDWIN8), 10.0.9.45(TDDESKTOP-DT), 10.0.9.65(MYCO30DEV), 10.0.9.74(BKRICKEY-WIN81), 10.0.9.95(MMAYHEMON-HP), 10.0.9.123(ISTCORP-PC)

Vulnerability Detection Result

Here is the list of DCE/RPC or MSRPC services running on this host via the TCP protocol: Port: 49152/tcp UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1 Endpoint: ncacn_ip_tcp:10.0.1.3[49152] Port: 49153/tcp UUID: 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1 Endpoint: ncacn_ip_tcp:10.0.1.3[49153] Annotation: NRP server endpoint UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1 Endpoint: ncacn_ip_tcp:10.0.1.3[49153] Annotation: DHCP Client LRPC Endpoint UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1 Endpoint: ncacn_ip_tcp:10.0.1.3[49153] Annotation: DHCPv6 Client LRPC Endpoint UUID: abfb6ca3-0c5e-4734-9285-0aee72fe8d1c, version 1 Endpoint: ncacn_ip_tcp:10.0.1.3[49153] Annotation: Wcm Service UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1 Endpoint: ncacn_ip_tcp:10.0.1.3[49153] Annotation: Event log TCPIP Port: 49154/tcp UUID: 1a0d010f-1c33-432c-b0f5-8cf4e8053099, version 1 Endpoint: ncacn_ip_tcp:10.0.1.3[49154] Annotation: IdSegSrv service UUID: 201ef99a-7fa0-444c-9399-19ba84f12a1a, version 1 Endpoint: ncacn_ip_tcp:10.0.1.3[49154] Annotation: AppInfo UUID: 2e6035b2-e8f1-41a7-a044-656b439c4c34, version 1 Endpoint: ncacn_ip_tcp:10.0.1.3[49154] Annotation: Proxy Manager provider server endpoint UUID: 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1 Endpoint: ncacn_ip_tcp:10.0.1.3[49154] UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1 Endpoint: ncacn_ip_tcp:10.0.1.3[49154] UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1 Endpoint: ncacn_ip_tcp:10.0.1.3[49154] Annotation: IP Transition Configuration endpoint UUID: 58e604e8-9adb-4d2e-a464-3b0683fb1480, version 1 Endpoint: ncacn_ip_tcp:10.0.1.3[49154] Annotation: AppInfo UUID: 5f54ce7d-5b79-4175-8584-cb65313a0e98, version 1 Endpoint: ncacn_ip_tcp:10.0.1.3[49154] Annotation: AppInfo UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1 Endpoint: ncacn_ip_tcp:10.0.1.3[49154] UUID: 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1 Endpoint: ncacn_ip_tcp:10.0.1.3[49154] Annotation: XactSrv service UUID: a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1 Endpoint: ncacn_ip_tcp:10.0.1.3[49154] Annotation: IKE/Authip API UUID: c36be077-e14b-4fe9-8abc-e856ef4f048b, version 1 Endpoint: ncacn_ip_tcp:10.0.1.3[49154] Annotation: Proxy Manager client server endpoint UUID: c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1 Endpoint: ncacn_ip_tcp:10.0.1.3[49154] Annotation: Adh APIs UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1 Endpoint: ncacn_ip_tcp:10.0.1.3[49154] Annotation: Impl friendly name UUID: fd7a0523-dc70-43dd-9b2e-9c5ed48225b1, version 1 Endpoint: ncacn_ip_tcp:10.0.1.3[49154] Annotation: AppInfo Port: 49155/tcp UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0 Endpoint: ncacn_ip_tcp:10.0.1.3[49155] Annotation: RemoteAccessCheck UUID: 12345678-1234-abcd-ef00-01234567cffb, version 1 Endpoint: ncacn_ip_tcp:10.0.1.3[49155] Named pipe : lsass Win32 service or process : Netlogon Description : Net Logon service UUID: 12345778-1234-abcd-ef00-0123456789ab, version 0 Endpoint: ncacn_ip_tcp:10.0.1.3[49155] Named pipe : lsass Win32 service or process : lsass.exe Description : LSA access UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1 Endpoint: ncacn_ip_tcp:10.0.1.3[49155] Named pipe : lsass Win32 service or process : lsass.exe Description : SAM access UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2 Endpoint: ncacn_ip_tcp:10.0.1.3[49155] Annotation: KeyIso UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1 Endpoint: ncacn_ip_tcp:10.0.1.3[49155] Annotation: Impl friendly name UUID: e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4 Endpoint: ncacn_ip_tcp:10.0.1.3[49155] Annotation: MS NT Directory DRS Interface Port: 49157/tcp UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0 Endpoint: ncacn_http:10.0.1.3[49157] Annotation: RemoteAccessCheck UUID: 12345678-1234-abcd-ef00-01234567cffb, version 1 Endpoint: ncacn_http:10.0.1.3[49157] Named pipe : lsass Win32 service or process : Netlogon Description : Net Logon service UUID: 12345778-1234-abcd-ef00-0123456789ab, version 0 Endpoint: ncacn_http:10.0.1.3[49157] Named pipe : lsass Win32 service or process : lsass.exe Description : LSA access UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1 Endpoint: ncacn_http:10.0.1.3[49157] Named pipe : lsass Win32 service or process : lsass.exe Description : SAM access UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2 Endpoint: ncacn_http:10.0.1.3[49157] Annotation: KeyIso UUID: e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4 Endpoint: ncacn_http:10.0.1.3[49157] Annotation: MS NT Directory DRS Interface Port: 49158/tcp UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0 Endpoint: ncacn_ip_tcp:10.0.1.3[49158] Annotation: RemoteAccessCheck UUID: 12345678-1234-abcd-ef00-01234567cffb, version 1 Endpoint: ncacn_ip_tcp:10.0.1.3[49158] Named pipe : lsass Win32 service or process : Netlogon Description : Net Logon service UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1 Endpoint: ncacn_ip_tcp:10.0.1.3[49158] Named pipe : lsass Win32 service or process : lsass.exe Description : SAM access UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2 Endpoint: ncacn_ip_tcp:10.0.1.3[49158] Annotation: KeyIso Port: 49159/tcp UUID: 0b6edbfa-4a24-4fc6-

8a23-942b1eca65d1, version 1 Endpoint: ncacn_ip_tcp:10.0.1.3[49159] UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1 Endpoint: ncacn_ip_tcp:10.0.1.3[49159] Named pipe : spoolss Win32 service or process : spoolsv.exe Description : Spooler service UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1 Endpoint: ncacn_ip_tcp:10.0.1.3[49159] UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1 Endpoint: ncacn_ip_tcp:10.0.1.3[49159] UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1 Endpoint: ncacn_ip_tcp:10.0.1.3[49159] Port: 49162/tcp UUID: 12d4b7c8-77d5-11d1-8c24-00c04fa3080d, version 1 Endpoint: ncacn_ip_tcp:10.0.1.3[49162] UUID: 3d267954-eeb7-11d1-b94e-00c04fa3080d, version 1 Endpoint: ncacn_ip_tcp:10.0.1.3[49162] Named pipe : HydraLsPipe Win32 service or process : lserver.exe Description : Terminal Server Licensing Port: 49163/tcp UUID: 5b821720-f63b-11d0-aad2-00c04fc324db, version 1 Endpoint: ncacn_ip_tcp:10.0.1.3[49163] UUID: 6bffd098-a112-3610-9833-46c3f874532d, version 1 Endpoint: ncacn_ip_tcp:10.0.1.3[49163] Port: 49174/tcp UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2 Endpoint: ncacn_ip_tcp:10.0.1.3[49174] Port: 49236/tcp UUID: 50abc2a4-574d-40b3-9d66-ee4fd5fba076, version 5 Endpoint: ncacn_ip_tcp:10.0.1.3[49236] Named pipe : dnsserver Win32 service or process : dns.exe Description : DNS Server Port: 49245/tcp UUID: 897e2e5f-93f3-4376-9c9c-fd2277495c27, version 1 Endpoint: ncacn_ip_tcp:10.0.1.3[49245] Annotation: Frs2 Service Note: DCE/RPC or MSRPC services running on this host locally were identified. Reporting this list is not enabled by default due to the possible large size of this list. See the script preferences to enable this reporting.
Multiple results by host

Impact
An attacker may use this fact to gain more knowledge about the remote host.

Solution
Filter incoming traffic to this ports.

Vulnerability Detection Method
Details: DCE/RPC and MSRPC Services Enumeration Reporting (OID: 1.3.6.1.4.1.25623.1.0.10736) Version used: $Revision: 6319 $

2.8 - Jenkins 2.93 XSS Vulnerability (Windows)

L	**Low**: (CVSS: 3.5) **OID:** 1.3.6.1.4.1.25623.1.0.113064	8080/tcp (http-alt)

Summary
Jenkins through 2.93 is prone to an XSS vulnerability.

Affected Nodes
10.0.9.99

Vulnerability Detection Result
Installed version: 2.89.2 Fixed version: NoneAvailable

Impact
Successful exploitation would allow an authenticated attacker to expose other users malicious code.

Solution
No solution as of 7th December 2017. This will be updated once a solution is available.

Vulnerability Insight
An authenticated attacker can use a crafted tool name in a job configuration form to conduct XSS attacks.

Vulnerability Detection Method
The script checks if the vulnerable version is present on the target host. Details: Jenkins 2.93 XSS Vulnerability (Windows) (OID: 1.3.6.1.4.1.25623.1.0.113064) Version used: $Revision: 8028 $

Product Detection Result
Product: cpe:/a:cloudbees:jenkins:2.89.2 Method: Jenkins CI Detection (OID: 1.3.6.1.4.1.25623.1.0.111001)

References
https://jenkins.io/changelog/