Internal

DOF Creations - Vulnerability Report

Report generated by Nessus™ Wed, 28 Jun 2023 23:27:15 EDT

TABLE OF CONTENTS

Overview

- Vulnerability Instances: all and exploitable, by severity..... 5

Top 10 Critical Vulnerabilities

- Top 10 Critical Vulnerabilities: (VPR)..... 7
- Top 10 Critical Vulnerabilities: (CVSS v3.0)..... 8

Top 10 High Vulnerabilities

- Top 10 High Vulnerabilities: (VPR)..... 10
- Top 10 High Vulnerabilities: (CVSS v3.0)..... 11

Top 10 Most Prevalent Vulnerabilities

- Top 10 Most Prevalent Vulnerabilities: (VPR)..... 13
- Top 10 Most Prevalent Vulnerabilities: (CVSS v3.0)..... 14

OS Detections Report

- OS Detections: Counts by Confidence Level..... 16
- OS Detections: Max Severity by OS Family (Confidence > 50)..... 17
- OS Detections: Details (Confidence > 50)..... 18

Unsupported Software Report

- No Results:..... 20

Default/Known Accounts Report

- Default/Known Accounts: Top 25..... 22
- Default/Known Accounts: Hosts by Plugin..... 23

Vulnerabilities by Host

- 192.168.192.1..... 25
- 192.168.192.104..... 27
- 192.168.192.116..... 28

- 192.168.192.117.....29
- 192.168.192.125.....30
- 192.168.192.126.....31
- 192.168.192.129.....33
- 192.168.192.130.....34
- 192.168.192.137.....35
- 192.168.192.138.....36
- 192.168.192.139.....37
- 192.168.192.140.....39
- 192.168.192.141.....41
- 192.168.192.146.....43
- 192.168.192.149.....44
- 192.168.192.151.....47
- 192.168.192.152.....48
- 192.168.192.153.....49
- 192.168.192.154.....51
- 192.168.192.155.....53
- 192.168.192.156.....56

Remediations

- Suggested Remediations.....59

Overview

The Overview section contains two matrices that provide summary counts, by severity, using VPR or CVSS. Within each cell there is a number for the vulnerability count, and in parentheses the count of exploitable vulnerabilities. Also provided is the count based on severity level.

Vulnerability Instances: all and exploitable, by severity

VPR: all(exploitable)

CVSS v3.0: all(exploitable)

Top 10 Critical Vulnerabilities

The two tables in this chapter provide a top 10 vulnerabilities grouped using the critical VPR or critical CVSS. For VPR and CVSS v3.0 the rating is 9.0 - 10, for CVSS v2.0 the rating is 10. The vulnerabilities identified using VPR are the most active in the wild, and based on an in-depth threat analysis, are considered the most critical to mitigate. Traditionally, the method for identifying risk was most commonly with CVSS v3.0 or CVSS v2.0. While each still remain very important, and should be mitigated, these vulnerabilities are not given the same context as VPR identified vulnerabilities.

Top 10 Critical Vulnerabilities: (VPR)

Top 10 most prevalent critical vulnerabilities

Plugin ID	Plugin Name	Plugin Family	VPR	Known Exploit?	Publication Date	Count
172186	Apache 2.4.x < 2.4.56 Multiple Vulnerabilities	Web Servers	9.4	-	2023/01/29	2

Top 10 Critical Vulnerabilities: (CVSS v3.0)

Top 10 most prevalent critical vulnerabilities

Plugin ID	Plugin Name	Plugin Family	CVSS v3.0	Known Exploit?	Publication Date	Count
156255	Apache 2.4.x >= 2.4.7 / < 2.4.52 Forward Proxy DoS / SSRF	Web Servers	9.8	Yes	2021/11/18	2
158900	Apache 2.4.x < 2.4.53 Multiple Vulnerabilities	Web Servers	9.8	-	2021/12/16	2
160477	OpenSSL 1.1.1 < 1.1.1o Vulnerability	Web Servers	9.8	-	2022/05/03	2
161454	Apache 2.4.x < 2.4.52 mod_lua Buffer Overflow	Web Servers	9.8	Yes	2021/11/18	2
161948	Apache 2.4.x < 2.4.54 Multiple Vulnerabilities	Web Servers	9.8	-	2022/03/02	2
162420	OpenSSL 1.1.1 < 1.1.1p Vulnerability	Web Servers	9.8	-	2022/06/21	2
172186	Apache 2.4.x < 2.4.56 Multiple Vulnerabilities	Web Servers	9.8	-	2023/01/29	2
170113	Apache 2.4.x < 2.4.55 Multiple Vulnerabilities	Web Servers	9.0	-	2022/07/12	2
64394	Portable SDK for UPnP Devices (libupnp) < 1.6.18 Multiple Stack-based Buffer Overflows RCE	Gain a shell remotely	9.8	Yes	2012/03/08	1

* indicates the v3.0 score was not available; the v2.0 score is shown

Top 10 High Vulnerabilities

The two tables in this chapter provide a top ' + limit + ' vulnerabilities grouped using the High VPR or High CVSS. For VPR and CVSS v3.0 the rating is 7.0 - 8.9, for CVSS v2.0 the rating is 7.0 - 9.9. The vulnerabilities identified using VPR are the most active in the wild and based on an in-depth threat analysis are considered the most critical to mitigate. Traditionally, the method for identifying risk was most commonly with CVSS v3.0 or CVSS v2.0. While each still remain very important, and should be mitigated, these vulnerabilities are not given the same context as VPR identified vulnerabilities.

Top 10 High Vulnerabilities: (VPR)

Top 10 most prevalent high vulnerabilities

Plugin ID	Plugin Name	Plugin Family	VPR	Known Exploit?	Publication Date	Count
156255	Apache 2.4.x >= 2.4.7 / < 2.4.52 Forward Proxy DoS / SSRF	Web Servers	8.4	Yes	2021/11/18	2
161454	Apache 2.4.x < 2.4.52 mod_lua Buffer Overflow	Web Servers	8.4	Yes	2021/11/18	2
158900	Apache 2.4.x < 2.4.53 Multiple Vulnerabilities	Web Servers	7.4	-	2021/12/16	2
160477	OpenSSL 1.1.1 < 1.1.1o Vulnerability	Web Servers	7.4	-	2022/05/03	2
161948	Apache 2.4.x < 2.4.54 Multiple Vulnerabilities	Web Servers	7.4	-	2022/03/02	2
162420	OpenSSL 1.1.1 < 1.1.1p Vulnerability	Web Servers	7.4	-	2022/06/21	2
170113	Apache 2.4.x < 2.4.55 Multiple Vulnerabilities	Web Servers	7.3	-	2022/07/12	2
64394	Portable SDK for UPnP Devices (libupnp) < 1.6.18 Multiple Stack-based Buffer Overflows RCE	Gain a shell remotely	7.4	Yes	2012/03/08	1

Top 10 High Vulnerabilities: (CVSS v3.0)

Top 10 most prevalent high vulnerabilities

Plugin ID	Plugin Name	Plugin Family	CVSS v3.0	Known Exploit?	Publication Date	Count
42873	SSL Medium Strength Cipher Suites Supported (SWEET32)	General	7.5	-	2016/08/24	3
158974	OpenSSL 1.1.1 < 1.1.1n Vulnerability	Web Servers	7.5	Yes	2022/03/15	2
171079	OpenSSL 1.1.1 < 1.1.1t Multiple Vulnerabilities	Web Servers	7.4	-	2023/02/07	2
35291	SSL Certificate Signed Using Weak Hashing Algorithm	General	7.5	Yes	2004/08/18	1

* indicates the v3.0 score was not available; the v2.0 score is shown

Top 10 Most Prevalent Vulnerabilities

The two tables in this chapter provide a top 10 vulnerabilities grouped using the Medium through Critical. For VPR, CVSS v3.0, and CVSS v2.0 the rating is 4.0 - 10. The vulnerabilities identified using VPR are the most active in the wild and based on an in-depth threat analysis are considered the most critical to mitigate. Traditionally, the method for identifying risk was most commonly with CVSS v3.0 or CVSS v2.0. While each still remain very important, and should be mitigated, these vulnerabilities are not given the same context as VPR identified vulnerabilities.

Top 10 Most Prevalent Vulnerabilities: (VPR)

Top 10 most prevalent (medium, high, critical) vulnerabilities

Plugin ID	Plugin Name	Plugin Family	VPR	Known Exploit?	Publication Date	Count
42873	SSL Medium Strength Cipher Suites Supported (SWEET32)	General	6.1	-	2016/08/24	3
172186	Apache 2.4.x < 2.4.56 Multiple Vulnerabilities	Web Servers	9.4	-	2023/01/29	2
156255	Apache 2.4.x >= 2.4.7 / < 2.4.52 Forward Proxy DoS / SSRF	Web Servers	8.4	Yes	2021/11/18	2
161454	Apache 2.4.x < 2.4.52 mod_lua Buffer Overflow	Web Servers	8.4	Yes	2021/11/18	2
158900	Apache 2.4.x < 2.4.53 Multiple Vulnerabilities	Web Servers	7.4	-	2021/12/16	2
160477	OpenSSL 1.1.1 < 1.1.1o Vulnerability	Web Servers	7.4	-	2022/05/03	2
161948	Apache 2.4.x < 2.4.54 Multiple Vulnerabilities	Web Servers	7.4	-	2022/03/02	2
162420	OpenSSL 1.1.1 < 1.1.1p Vulnerability	Web Servers	7.4	-	2022/06/21	2
170113	Apache 2.4.x < 2.4.55 Multiple Vulnerabilities	Web Servers	7.3	-	2022/07/12	2
171079	OpenSSL 1.1.1 < 1.1.1t Multiple Vulnerabilities	Web Servers	6.7	-	2023/02/07	2

Top 10 Most Prevalent Vulnerabilities: (CVSS v3.0)

Top 10 most prevalent (medium, high, critical) vulnerabilities

Plugin ID	Plugin Name	Plugin Family	CVSS v3.0	Known Exploit?	Publication Date	Count
51192	SSL Certificate Cannot Be Trusted	General	6.5	-	2010/12/15	11
57582	SSL Self-Signed Certificate	General	6.5	-	2012/01/17	6
134220	nginx < 1.17.7 Information Disclosure	Web Servers	5.3	-	2019/12/24	4
42873	SSL Medium Strength Cipher Suites Supported (SWEET32)	General	7.5	-	2016/08/24	3
156255	Apache 2.4.x >= 2.4.7 / < 2.4.52 Forward Proxy DoS / SSRF	Web Servers	9.8	Yes	2021/11/18	2
158900	Apache 2.4.x < 2.4.53 Multiple Vulnerabilities	Web Servers	9.8	-	2021/12/16	2
160477	OpenSSL 1.1.1 < 1.1.1o Vulnerability	Web Servers	9.8	-	2022/05/03	2
161454	Apache 2.4.x < 2.4.52 mod_lua Buffer Overflow	Web Servers	9.8	Yes	2021/11/18	2
161948	Apache 2.4.x < 2.4.54 Multiple Vulnerabilities	Web Servers	9.8	-	2022/03/02	2
162420	OpenSSL 1.1.1 < 1.1.1p Vulnerability	Web Servers	9.8	-	2022/06/21	2

* indicates the v3.0 score was not available; the v2.0 score is shown

OS Detections Report

System administrators and the security team work together to identify systems at the most risk. A good first step is to understand the operating systems in the network. This report provides a summary of the most prevalent operating systems on the network.

OS Detections: Counts by Confidence Level

Nessus leverages several attributes such as "operating-system", "operating-system-unsupported", "os" and "operating-system-conf" to group the hosts into different OS families. In doing so this report organizes the system counts first using a matrix style table, that displays rows by the confidence level and then by an OS family using columns. The All column displays the total count of plugin present at the respective Confidence Level. The Windows, MacOS, and Linux, columns filter based on the key words "windows", "mac", or "linux". The Other column will match on anything that does match the aforementioned key words.

Confidence	All	Windows	MacOS	Linux	Other
0 - 9	0	0	0	0	0
10 - 19	0	0	0	0	0
20 - 29	0	0	0	0	0
30 - 39	0	0	0	0	0
40 - 49	0	0	0	0	0
50 - 59	1	0	0	1	0
60 - 69	3	0	0	3	0
70 - 79	4	1	0	1	2
80 - 89	0	0	0	0	0
90 - 100	7	0	1	2	4
Totals	15	1	1	7	6

OS Detections: Max Severity by OS Family (Confidence > 50)

Building upon the previous matrix, the OS Detections: Max Severity by OS Family (Confidence > 50) table provides the security team with summary view of risk based on operating system. The counts represented in this table are based on system count by OS family and if a vulnerability with the indicated severity is present. For example, in the Windows column and the High severity row, say there is a number 15. The number represents that there are 15 assets identified to have a Windows operating system with at least 1 high severity vulnerability.

Severity (CVSS v3.0)	All	Windows	MacOS	Linux	Other
CRITICAL	2	0	0	1	1
HIGH	2	0	0	2	0
MEDIUM	5	0	0	4	1
LOW	0	0	0	0	0
INFO	6	1	1	0	4
Totals	15	1	1	7	6

OS Detections: Details (Confidence > 50)

The OS Detections: Details (Confidence > 50) table presents all of the OS family detections, along with assets within each OS. The table also displays if the OS is supported by the vendor.

OS	Count	Unsupportec	Hosts
Linux Kernel 2.6	3	no	192.168.192.141, 192.168.192.139, 192.168.192.126
Nutanix	3	no	192.168.192.155, 192.168.192.154, 192.168.192.153
Debian 7.0 Linux Kernel 3.2	1	no	192.168.192.140
FreeBSD 13.1-RELEASE-p5 (amd64)	1	no	192.168.192.1
Linux Kernel 4.15 on Ubuntu 18.04 (bionic)	1	no	192.168.192.156
Linux Kernel 6.1.0-kali9-amd64	1	no	192.168.192.149
Microsoft Windows 10	1	no	192.168.192.104
an operating system associated with Nest Labs Inc.	1	no	192.168.192.138
an operating system associated with Nintendo Co.,Ltd	1	no	192.168.192.117
an operating system associated with Sony Interactive Entertainment Inc.	1	no	192.168.192.130
iPhone or iPad	1	no	192.168.192.116

Unsupported Software Report

The proliferation of unsupported and end-of-life (EOL) software is an issue for many organizations and increases the effort required to minimize risk. As software reaches end-of-life, vendors often stop providing updates and support for the older versions. This report provides system administrators with a summary of the software that is no longer supported and puts the organization at the most risk.

No Results:

No Unsupported Software Found

Default/Known Accounts Report

Default and/or known accounts create an easy entry point for attackers to take advantage of to gain access to the network and hosts. Once inside the network, an attacker can perform malicious attacks, steal sensitive data, and cause significant damage to critical systems. This report provides a summary of the most prevalent detections of default and known accounts.

Default/Known Accounts: Top 25

The Default/Known Accounts: Top 25 table uses the a list of plugins that are known to detect default and known accounts. The data is then sorted using the count, which is a representation of the affected hosts. While some plugins may be present more than one time on a single host, for the most part a plugin will only be present once on each host. This list of vulnerabilities exposes the organization to many different attach frameworks and script kiddie attacks. These vulnerabilities should be prioritized and the software removed or updated to a supported version as soon as possible.

Severity (CVSS v3.0)	Plugin ID	Plugin Name	Count
INFO	95928	Linux User List Enumeration	1

Default/Known Accounts: Hosts by Plugin

The Default/Known Accounts: Hosts by Plugin table provides the IT operations team with an action plan and the identified hosts for each vulnerability. IT managers are able to use this information in planning patch deployments and in working with the information security team in risk mitigation efforts. The table also uses a known list of plugins that identify entities that are using default and/or known accounts and then sorts the scan results using severity, then plugin ID. The entries in the "Hosts" column are then sorted in ascending order.

Severity (CVSS v3.0)	Plugin ID	Plugin Name	Hosts
INFO	95928	Linux User List Enumeration	192.168.192.149

Vulnerabilities by Host

192.168.192.1

Vulnerabilities Total: 42

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate
MEDIUM	5.8	-	97861	Network Time Protocol (NTP) Mode 6 Scanner
MEDIUM	5.3	-	15901	SSL Certificate Expiry
MEDIUM	5.3	-	45411	SSL Certificate with Wrong Hostname
LOW	3.3*	-	10663	DHCP Server Detection
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	46180	Additional DNS Hostnames
INFO	N/A	-	166602	Asset Attribute: Fully Qualified Domain Name (FQDN)
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	11002	DNS Server Detection
INFO	N/A	-	72779	DNS Server Version Detection
INFO	N/A	-	35371	DNS Server hostname.bind Map Hostname Disclosure
INFO	N/A	-	54615	Device Type
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	84502	HSTS Missing From HTTPS Server
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	85805	HTTP/2 Cleartext Detection

INFO	N/A	-	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	11935	IPSEC Internet Key Exchange (IKE) Version 1 Detection
INFO	N/A	-	62695	IPSEC Internet Key Exchange (IKE) Version 2 Detection
INFO	N/A	-	106658	JQuery Detection
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	10884	Network Time Protocol (NTP) Server Detection
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	45410	SSL Certificate 'commonName' Mismatch
INFO	N/A	-	10863	SSL Certificate Information
INFO	N/A	-	21643	SSL Cipher Suites Supported
INFO	N/A	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	84821	TLS ALPN Supported Protocol Enumeration
INFO	N/A	-	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	-	138330	TLS Version 1.3 Protocol Detection
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	87872	Unbound DNS Resolver Remote Version Detection
INFO	N/A	-	100669	Web Application Cookies Are Expired
INFO	N/A	-	10386	Web Server No 404 Error Code Check

* indicates the v3.0 score was not available; the v2.0 score is shown

192.168.192.104

Vulnerabilities Total: 16

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	54615	Device Type
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	43111	HTTP Methods Allowed (per directory)
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	53513	Link-Local Multicast Name Resolution (LLMNR) Detection
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	20301	VMware ESX/GSX Server detection
INFO	N/A	-	66717	mDNS Detection (Local Network)

* indicates the v3.0 score was not available; the v2.0 score is shown

192.168.192.116

Vulnerabilities Total: 7

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
INFO	N/A	-	54615	Device Type
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	10919	Open Port Re-check
INFO	N/A	-	10287	Traceroute Information

* indicates the v3.0 score was not available; the v2.0 score is shown

192.168.192.117

Vulnerabilities Total: 7

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
INFO	N/A	-	54615	Device Type
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	102821	OS Identification : OUI
INFO	N/A	-	10287	Traceroute Information

* indicates the v3.0 score was not available; the v2.0 score is shown

192.168.192.125

Vulnerabilities Total: 5

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	66717	mDNS Detection (Local Network)

* indicates the v3.0 score was not available; the v2.0 score is shown

192.168.192.126

1	2	5	0	28
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 36

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	7.4	64394	Portable SDK for UPnP Devices (libupnp) < 1.6.18 Multiple Stack-based Buffer Overflows RCE
HIGH	7.5	5.1	35291	SSL Certificate Signed Using Weak Hashing Algorithm
HIGH	7.5	6.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	-	157288	TLS Version 1.1 Protocol Deprecated
MEDIUM	5.9	3.6	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	54615	Device Type
INFO	N/A	-	19689	Embedded Web Server Detection
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	84502	HSTS Missing From HTTPS Server
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information

INFO	N/A	-	11936	OS Identification
INFO	N/A	-	10919	Open Port Re-check
INFO	N/A	-	50845	OpenSSL Detection
INFO	N/A	-	66334	Patch Report
INFO	N/A	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	10863	SSL Certificate Information
INFO	N/A	-	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	21643	SSL Cipher Suites Supported
INFO	N/A	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	87242	TLS NPN Supported Protocol Enumeration
INFO	N/A	-	62564	TLS Next Protocols Supported
INFO	N/A	-	121010	TLS Version 1.1 Protocol Detection
INFO	N/A	-	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	35711	Universal Plug and Play (UPnP) Protocol Detection

* indicates the v3.0 score was not available; the v2.0 score is shown

192.168.192.129

Vulnerabilities Total: 5

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	66717	mDNS Detection (Local Network)

* indicates the v3.0 score was not available; the v2.0 score is shown

192.168.192.130

Vulnerabilities Total: 9

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	54615	Device Type
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	102821	OS Identification : OUI
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	66717	mDNS Detection (Local Network)

* indicates the v3.0 score was not available; the v2.0 score is shown

192.168.192.137

Vulnerabilities Total: 4

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	10287	Traceroute Information

* indicates the v3.0 score was not available; the v2.0 score is shown

192.168.192.138

Vulnerabilities Total: 7

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
INFO	N/A	-	54615	Device Type
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	102821	OS Identification : OUI
INFO	N/A	-	10287	Traceroute Information

* indicates the v3.0 score was not available; the v2.0 score is shown

192.168.192.139

Vulnerabilities Total: 28

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
HIGH	7.5	6.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	54615	Device Type
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	83298	SSL Certificate Chain Contains Certificates Expiring Soon
INFO	N/A	-	42981	SSL Certificate Expiry - Future Expiry
INFO	N/A	-	10863	SSL Certificate Information
INFO	N/A	-	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	21643	SSL Cipher Suites Supported
INFO	N/A	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported

INFO	N/A	-	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	-	138330	TLS Version 1.3 Protocol Detection
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	35711	Universal Plug and Play (UPnP) Protocol Detection
INFO	N/A	-	11154	Unknown Service Detection: Banner Retrieval
INFO	N/A	-	35712	Web Server UPnP Detection

* indicates the v3.0 score was not available; the v2.0 score is shown

192.168.192.140

Vulnerabilities Total: 19

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
MEDIUM	6.5	4.0	50686	IP Forwarding Enabled
LOW	3.7	-	153953	SSH Weak Key Exchange Algorithms Enabled
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	54615	Device Type
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	70657	SSH Algorithms and Languages Supported
INFO	N/A	-	149334	SSH Password Authentication Accepted
INFO	N/A	-	153588	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	-	10267	SSH Server Type and Version Information
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided

INFO	N/A	-	10287	Traceroute Information

* indicates the v3.0 score was not available; the v2.0 score is shown

192.168.192.141

0	1	2	0	25
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 28

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
HIGH	7.5	6.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	54615	Device Type
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	83298	SSL Certificate Chain Contains Certificates Expiring Soon
INFO	N/A	-	42981	SSL Certificate Expiry - Future Expiry
INFO	N/A	-	10863	SSL Certificate Information
INFO	N/A	-	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	21643	SSL Cipher Suites Supported
INFO	N/A	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported

INFO	N/A	-	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	-	138330	TLS Version 1.3 Protocol Detection
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	35711	Universal Plug and Play (UPnP) Protocol Detection
INFO	N/A	-	11154	Unknown Service Detection: Banner Retrieval
INFO	N/A	-	35712	Web Server UPnP Detection

* indicates the v3.0 score was not available; the v2.0 score is shown

192.168.192.146

Vulnerabilities Total: 4

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	10287	Traceroute Information

* indicates the v3.0 score was not available; the v2.0 score is shown

192.168.192.149

Vulnerabilities Total: 48

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
INFO	N/A	-	141394	Apache HTTP Server Installed (Linux)
INFO	N/A	-	142640	Apache HTTP Server Site Enumeration
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	55472	Device Hostname
INFO	N/A	-	54615	Device Type
INFO	N/A	-	25203	Enumerate IPv4 Interfaces via SSH
INFO	N/A	-	25202	Enumerate IPv6 Interfaces via SSH
INFO	N/A	-	33276	Enumerate MAC Addresses via SSH
INFO	N/A	-	170170	Enumerate the Network Interaface configuration via SSH
INFO	N/A	-	168980	Enumerate the PATH Variables
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	171410	IP Assignment Method Detection
INFO	N/A	-	147817	Java Detection and Identification (Linux / Unix)
INFO	N/A	-	151883	Libgcrypt Installed (Linux/UNIX)
INFO	N/A	-	157358	Linux Mounted Devices

INFO	N/A	-	95928	Linux User List Enumeration
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	10147	Nessus Server Detection
INFO	N/A	-	64582	Netstat Connection Information
INFO	N/A	-	14272	Netstat Portscanner (SSH)
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	97993	OS Identification and Installed Software Enumeration over SSH v2 (Using New SSH Library)
INFO	N/A	-	117887	OS Security Patch Assessment Available
INFO	N/A	-	148373	OpenJDK Java Detection (Linux / Unix)
INFO	N/A	-	168007	OpenSSL Installed (Linux)
INFO	N/A	-	130024	PostgreSQL Client/Server Installed (Linux)
INFO	N/A	-	45405	Reachable IPv6 address
INFO	N/A	-	174788	SQLite Local Detection (Linux)
INFO	N/A	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	10863	SSL Certificate Information
INFO	N/A	-	21643	SSL Cipher Suites Supported
INFO	N/A	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	22869	Software Enumeration (SSH)
INFO	N/A	-	42822	Strict Transport Security (STS) Detection
INFO	N/A	-	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	-	110095	Target Credential Issues by Authentication Protocol - No Issues Found
INFO	N/A	-	141118	Target Credential Status by Authentication Protocol - Valid Credentials Provided
INFO	N/A	-	163326	Tenable Nessus Installed (Linux)

INFO	N/A	-	56468	Time of Last System Startup
INFO	N/A	-	110483	Unix / Linux Running Processes Information
INFO	N/A	-	152742	Unix Software Discovery Commands Available
INFO	N/A	-	20094	VMware Virtual Machine Detection
INFO	N/A	-	136340	nginx Installed (Linux/UNIX)

* indicates the v3.0 score was not available; the v2.0 score is shown

192.168.192.151

Vulnerabilities Total: 6

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	66717	mDNS Detection (Local Network)

* indicates the v3.0 score was not available; the v2.0 score is shown

192.168.192.152

Vulnerabilities Total: 5

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	20094	VMware Virtual Machine Detection

* indicates the v3.0 score was not available; the v2.0 score is shown

192.168.192.153

Vulnerabilities Total: 36

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	48204	Apache HTTP Server Version
INFO	N/A	-	39521	Backported Security Patch Detection (WWW)
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	54615	Device Type
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	84502	HSTS Missing From HTTPS Server
INFO	N/A	-	43111	HTTP Methods Allowed (per directory)
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	132584	Palo Alto Expedition Web Detection
INFO	N/A	-	70657	SSH Algorithms and Languages Supported

INFO	N/A	-	149334	SSH Password Authentication Accepted
INFO	N/A	-	10881	SSH Protocol Versions Supported
INFO	N/A	-	153588	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	-	10267	SSH Server Type and Version Information
INFO	N/A	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	10863	SSL Certificate Information
INFO	N/A	-	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	21643	SSL Cipher Suites Supported
INFO	N/A	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	-	138330	TLS Version 1.3 Protocol Detection
INFO	N/A	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	20094	VMware Virtual Machine Detection

* indicates the v3.0 score was not available; the v2.0 score is shown

192.168.192.154

0	0	0	0	22
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 22

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	54615	Device Type
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	122364	Python Remote HTTP Detection
INFO	N/A	-	70657	SSH Algorithms and Languages Supported
INFO	N/A	-	149334	SSH Password Authentication Accepted
INFO	N/A	-	10881	SSH Protocol Versions Supported
INFO	N/A	-	153588	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	-	10267	SSH Server Type and Version Information
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	25220	TCP/IP Timestamps Supported

INFO	N/A	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	20094	VMware Virtual Machine Detection

* indicates the v3.0 score was not available; the v2.0 score is shown

192.168.192.155

Vulnerabilities Total: 51

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	8.4	161454	Apache 2.4.x < 2.4.52 mod_lua Buffer Overflow
CRITICAL	9.8	7.4	158900	Apache 2.4.x < 2.4.53 Multiple Vulnerabilities
CRITICAL	9.8	7.4	161948	Apache 2.4.x < 2.4.54 Multiple Vulnerabilities
CRITICAL	9.8	9.4	172186	Apache 2.4.x < 2.4.56 Multiple Vulnerabilities
CRITICAL	9.8	8.4	156255	Apache 2.4.x >= 2.4.7 / < 2.4.52 Forward Proxy DoS / SSRF
CRITICAL	9.8	7.4	160477	OpenSSL 1.1.1 < 1.1.1o Vulnerability
CRITICAL	9.8	7.4	162420	OpenSSL 1.1.1 < 1.1.1p Vulnerability
CRITICAL	9.0	7.3	170113	Apache 2.4.x < 2.4.55 Multiple Vulnerabilities
HIGH	7.5	5.1	158974	OpenSSL 1.1.1 < 1.1.1n Vulnerability
HIGH	7.4	6.7	171079	OpenSSL 1.1.1 < 1.1.1t Multiple Vulnerabilities
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate
MEDIUM	5.9	4.4	157228	OpenSSL 1.1.1 < 1.1.1m Vulnerability
MEDIUM	5.3	4.0	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.3	2.9	162721	OpenSSL 1.1.1 < 1.1.1q Vulnerability
MEDIUM	5.3	4.4	173260	OpenSSL 1.1.1 < 1.1.1u Multiple Vulnerabilities
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	48204	Apache HTTP Server Version
INFO	N/A	-	45590	Common Platform Enumeration (CPE)

INFO	N/A	-	54615	Device Type
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	84502	HSTS Missing From HTTPS Server
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	57323	OpenSSL Version Detection
INFO	N/A	-	66334	Patch Report
INFO	N/A	-	122364	Python Remote HTTP Detection
INFO	N/A	-	70657	SSH Algorithms and Languages Supported
INFO	N/A	-	149334	SSH Password Authentication Accepted
INFO	N/A	-	10881	SSH Protocol Versions Supported
INFO	N/A	-	153588	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	-	10267	SSH Server Type and Version Information
INFO	N/A	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	10863	SSL Certificate Information
INFO	N/A	-	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	21643	SSL Cipher Suites Supported
INFO	N/A	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	94761	SSL Root Certification Authority Certificate Information
INFO	N/A	-	156899	SSL/TLS Recommended Cipher Suites

INFO	N/A	-	22964	Service Detection
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	-	138330	TLS Version 1.3 Protocol Detection
INFO	N/A	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	20094	VMware Virtual Machine Detection

* indicates the v3.0 score was not available; the v2.0 score is shown

192.168.192.156

Vulnerabilities Total: 30

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
MEDIUM	6.1	5.7	136929	JQuery 1.2 < 3.5.0 Multiple XSS
MEDIUM	5.3	2.2	134220	nginx < 1.17.7 Information Disclosure
MEDIUM	5.3	-	121479	web.config File Information Disclosure
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	54615	Device Type
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	106658	JQuery Detection
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	66334	Patch Report
INFO	N/A	-	70657	SSH Algorithms and Languages Supported
INFO	N/A	-	149334	SSH Password Authentication Accepted
INFO	N/A	-	10881	SSH Protocol Versions Supported

INFO	N/A	-	153588	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	-	10267	SSH Server Type and Version Information
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	20094	VMware Virtual Machine Detection
INFO	N/A	-	100669	Web Application Cookies Are Expired
INFO	N/A	-	10386	Web Server No 404 Error Code Check
INFO	N/A	-	10302	Web Server robots.txt Information Disclosure
INFO	N/A	-	106375	nginx HTTP Server Detection

* indicates the v3.0 score was not available; the v2.0 score is shown

Remediations

Suggested Remediations

Taking the following actions across 1 hosts would resolve 25% of the vulnerabilities on the network.

ACTION TO TAKE	VULNS	HOSTS
Apache 2.4.x < 2.4.56 Multiple Vulnerabilities: Upgrade to Apache version 2.4.56 or later.	19	1
OpenSSL 1.1.1 < 1.1.1u Multiple Vulnerabilities: Upgrade to OpenSSL version 1.1.1u or later.	9	1