Vulnerability Report

193.136.172.10 - Celeborn.ua.pt

name: Celeborn.ua.pt
ports: {'open': {'1720': {'type': 'tcp', 'state': 'open', 'service': 'h323q931?', 'version': ''}}, 'Filtered': ' 999 filtered tcp ports '}
OS: OpenBSD 4.0
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', 'celeborn.ua.pt': '193.136.172.10'}
Rating: 0

193.136.173.34 - abc.ua.pt

name: abc.ua.pt
ports: {'open': {'1720': {'type': 'tcp', 'state': 'open', 'service': 'h323q931?', 'version': ''}}, 'Filtered': ' 999 filtered tcp ports '}
OS: OpenBSD 4.0
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', 'abc.ua.pt': '193.136.173.34'}
Rating: 0

193.136.172.209 - absolut.ua.pt

name: absolut.ua.pt
ports: {'open': {'1720': {'type': 'tcp', 'state': 'open', 'service': 'h323q931?', 'version': ''}, '2179': {'type': 'tcp', 'state': 'closed', 'service': 'vmrdp', 'version': ''}}, 'Filtered': ' 998 filtered tcp ports '}
OS: OpenBSD 4.0
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', '10.1.0.92': '10.1.0.92', 'fw-vsdc.ua.pt': '193.137.173.236', 'absolut.ua.pt': '193.136.172.209'}
Rating: 0

193.137.172.90 - aim.ua.pt

name: aim.ua.pt
ports: {'open': {'22': {'type': 'tcp', 'state': 'open', 'service': 'ssh', 'version': 'OpenSSHfor_Windows_8.1(protocol2.0)'}}, 'Filtered': ' 999 filtered tcp ports '}
OS: Microsoft Windows XP SP3
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', '10.1.0.92': '10.1.0.92', 'aim.ua.pt': '193.137.172.90'}

CVE-2012-0814

cvss: 3.5
severity: Low
cwe: CWE-255
cvss-vector: AV:N/AC:M/Au:S/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'SINGLE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}
Rating: 3.5

193.137.172.30 - alfresco.dev.ua.pt

name: alfresco.dev.ua.pt
ports: {'open': {}, 'Filtered': ' 1000 filtered tcp ports '}
OS:
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', '10.1.0.92': '10.1.0.92', 'dev-alfresco.ua.pt': '193.137.172.30'}
Rating: 0

193.136.172.184 - app.web.ua.pt

name: app.web.ua.pt
ports: {'open': {'1720': {'type': 'tcp', 'state': 'open', 'service': 'h323q931?', 'version': ''}}, 'Filtered': ' 999 filtered tcp ports '}
OS: OpenBSD 4.0
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', 'webapp.servers.ua.pt': '193.136.172.184'}
Rating: 0

192.168.248.164 - biobank.web.ua.pt

name: biobank.web.ua.pt
ports: {'open': {}, 'Filtered': ' 1000 filtered tcp ports '}
OS:
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', '10.1.0.92': '10.1.0.92', 'biobank.web.ua.pt': '192.168.248.164'}

Rating: 0

193.136.173.9 - blogs.ua.pt

name: blogs.ua.pt
ports: {'open': {'80': {'type': 'tcp', 'state': 'open', 'service': 'http', 'version': 'Apachehttpd'}, '443': {'type': 'tcp', 'state': 'open', 'service': 'ssl/http', 'version': 'Apachehttpd'}, '1720': {'type': 'tcp', 'state': 'open', 'service': 'h323q931?', 'version': ''}, '8000': {'type': 'tcp', 'state': 'open', 'service': 'http', 'version': 'HandleSystemProxyServer'}, '8001': {'type': 'tcp', 'state': 'closed', 'service': 'vcom-tunnel', 'version': ''}}, 'Filtered': ' 995 filtered tcp ports '}
OS:
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', '10.1.0.92': '10.1.0.92', 'fw-vsdc.ua.pt': '193.137.173.236', 'web-li.ua.pt': '193.136.173.9'}

CVE-2001-0131

cvss: 3.3
severity: Low
cwe: CWE-59
cvss-vector: AV:L/AC:M/Au:N/C:N/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'LOCAL'}

CVE-2002-0563

cvss: 5.0
severity: Medium
cwe: CWE-287
cvss-vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2008-1327

cvss: 7.5
severity: High
cwe: CWE-287
cvss-vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2009-0038

cvss: 4.3
severity: Medium
cwe: CWE-79
cvss-vector: AV:N/AC:M/Au:N/C:N/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'NONE', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2010-3449

cvss: 6.8
severity: Medium
cwe: CWE-352
cvss-vector: AV:N/AC:M/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2011-0533

cvss: 4.3
severity: Medium
cwe: CWE-79
cvss-vector: AV:N/AC:M/Au:N/C:N/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'NONE', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2013-0340

cvss: 6.8
severity: Medium
cwe: CWE-611
cvss-vector: AV:N/AC:M/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2014-0085

cvss: 2.1
severity: Low
cwe: CWE-255
cvss-vector: AV:L/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'LOCAL'}

CVE-2014-6271

cvss: 10.0
severity: Critical
cwe: CWE-78
cvss-vector: AV:N/AC:L/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2015-8982

cvss: 6.8
severity: Medium
cwe: CWE-190
cvss-vector: AV:N/AC:M/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2016-1234

cvss: 5.0
severity: Medium
cwe: CWE-119
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2016-2166

cvss: 5.8
severity: Medium
cwe: CWE-200
cvss-vector: AV:N/AC:M/Au:N/C:P/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2016-4462

cvss: 6.5
severity: Medium
cwe: CWE-20
cvss-vector: AV:N/AC:L/Au:S/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'SINGLE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2016-5387

cvss: 5.1
severity: Medium
cwe: CWE-284
cvss-vector: AV:N/AC:H/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'HIGH', 'vector': 'NETWORK'}

CVE-2016-5388

cvss: 5.1
severity: Medium
cwe: CWE-284
cvss-vector: AV:N/AC:H/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'HIGH', 'vector': 'NETWORK'}

CVE-2016-5582

cvss: 9.3
severity: Critical
cwe: CWE-284
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2016-6799

cvss: 5.0
severity: Medium
cwe: CWE-532
cvss-vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2017-15714

cvss: 7.5
severity: High
cwe: CWE-74
cvss-vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2017-17837

cvss: 4.3
severity: Medium
cwe: CWE-79
cvss-vector: AV:N/AC:M/Au:N/C:N/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'NONE', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2018-11786

cvss: 9.0
severity: Critical
cwe: CWE-269
cvss-vector: AV:N/AC:L/Au:S/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'SINGLE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2018-1199

cvss: 5.0
severity: Medium
cwe: CWE-20
cvss-vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2018-1336

cvss: 5.0
severity: Medium
cwe: CWE-835
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2018-16890

cvss: 5.0
severity: Medium
cwe: CWE-125
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2018-8010

cvss: 2.1
severity: Low
cwe: CWE-611
cvss-vector: AV:L/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'LOCAL'}

CVE-2018-8039

cvss: 6.8
severity: Medium
cwe: CWE-755
cvss-vector: AV:N/AC:M/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2019-0224

cvss: 4.3
severity: Medium
cwe: CWE-79
cvss-vector: AV:N/AC:M/Au:N/C:N/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'NONE', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2019-11231

cvss: 5.0
severity: Medium
cwe: CWE-22
cvss-vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-12401

cvss: 5.0
severity: Medium
cwe: CWE-776
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-12405

cvss: 6.8
severity: Medium
cwe: CWE-287
cvss-vector: AV:N/AC:M/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2019-12409

cvss: 7.5
severity: High
cwe: CWE-434
cvss-vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-12418

cvss: 4.4
severity: Medium
cwe: CWE-522
cvss-vector: AV:L/AC:M/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'LOCAL'}

CVE-2019-13012

cvss: 5.0
severity: Medium
cwe: CWE-732
cvss-vector: AV:N/AC:L/Au:N/C:N/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'NONE', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-13050

cvss: 5.0
severity: Medium
cwe: CWE-295
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-13115

cvss: 5.8
severity: Medium
cwe: CWE-190
cvss-vector: AV:N/AC:M/Au:N/C:P/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2019-13565

cvss: 5.0
severity: Medium
cwe: NVD-CWE-noinfo
cvss-vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-16056

cvss: 5.0
severity: Medium
cwe: NVD-CWE-noinfo
cvss-vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-17560

cvss: 6.4
severity: Medium
cwe: CWE-295
cvss-vector: AV:N/AC:L/Au:N/C:P/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-17570

cvss: 7.5
severity: High
cwe: CWE-502
cvss-vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-3822

cvss: 7.5
severity: High
cwe: CWE-787
cvss-vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-9512

cvss: 7.8
severity: High
cwe: CWE-400
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-9514

cvss: 7.8
severity: High
cwe: CWE-770
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-9515

cvss: 7.8
severity: High
cwe: CWE-770
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-9517

cvss: 7.8
severity: High
cwe: CWE-770
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-9518

cvss: 7.8
severity: High
cwe: CWE-770
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-9853

cvss: 6.8
severity: Medium
cwe: CWE-116
cvss-vector: AV:N/AC:M/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2020-13925

cvss: 10.0
severity: Critical
cwe: CWE-78
cvss-vector: AV:N/AC:L/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2020-13926

cvss: 7.5
severity: High
cwe: CWE-89
cvss-vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2020-13932

cvss: 4.3
severity: Medium
cwe: CWE-79
cvss-vector: AV:N/AC:M/Au:N/C:N/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'NONE', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2020-13948

cvss: 6.5
severity: Medium
cwe: NVD-CWE-noinfo
cvss-vector: AV:N/AC:L/Au:S/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'SINGLE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2020-13952

cvss: 5.5
severity: Medium
cwe: NVD-CWE-noinfo
cvss-vector: AV:N/AC:L/Au:S/C:P/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'SINGLE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2020-14621

cvss: 5.0
severity: Medium
cwe: NVD-CWE-noinfo
cvss-vector: AV:N/AC:L/Au:N/C:N/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'NONE', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2020-1752

cvss: 3.7
severity: Low
cwe: CWE-416
cvss-vector: AV:L/AC:H/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'HIGH', 'vector': 'LOCAL'}

CVE-2020-25709

cvss: 5.0
severity: Medium
cwe: CWE-617
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2020-7760

cvss: 5.0
severity: Medium
cwe: CWE-400
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-22696

cvss: 5.0
severity: Medium
cwe: CWE-918
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-23336

cvss: 4.0
severity: Medium
cwe: CWE-444
cvss-vector: AV:N/AC:H/Au:N/C:N/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'HIGH', 'vector': 'NETWORK'}

CVE-2021-23937

cvss: 5.0
severity: Medium
cwe: CWE-20
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-26291

cvss: 6.4
severity: Medium
cwe: CWE-346
cvss-vector: AV:N/AC:L/Au:N/C:P/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-26558

cvss: 5.0
severity: Medium
cwe: CWE-502
cvss-vector: AV:N/AC:L/Au:N/C:N/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'NONE', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-30468

cvss: 5.0
severity: Medium
cwe: CWE-400
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-30638

cvss: 5.0
severity: Medium
cwe: CWE-200
cvss-vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-31522

cvss: 7.5
severity: High
cwe: CWE-470
cvss-vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-32626

cvss: 6.5
severity: Medium
cwe: CWE-787
cvss-vector: AV:N/AC:L/Au:S/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'SINGLE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-36774

cvss: 4.0
severity: Medium
cwe: CWE-668
cvss-vector: AV:N/AC:L/Au:S/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'SINGLE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-37136

cvss: 5.0
severity: Medium
cwe: CWE-400
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-37137

cvss: 5.0
severity: Medium
cwe: CWE-400
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-41571

cvss: 4.0
severity: Medium
cwe: CWE-20
cvss-vector: AV:N/AC:L/Au:S/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'SINGLE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-41616

cvss: 7.5
severity: High
cwe: CWE-502
cvss-vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-43297

cvss: 7.5
severity: High
cwe: CWE-502
cvss-vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-44228

cvss: 9.3
severity: Critical
cwe: CWE-502
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2021-45457

cvss: 5.0
severity: Medium
cwe: CWE-522
cvss-vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-45458

cvss: 5.0
severity: Medium
cwe: CWE-326
cvss-vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2022-22932

cvss: 5.0
severity: Medium
cwe: CWE-22
cvss-vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}
Rating: 10.0

192.92.133.35 - bookstack.dev.ua.pt

name: bookstack.dev.ua.pt
ports: {'open': {'1720': {'type': 'tcp', 'state': 'open', 'service': 'h323q931?', 'version': ''}}, 'Filtered': ' 999 filtered tcp ports '}
OS: OpenBSD 4.0
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', 'docker-web-li.dev.ua.pt': '192.92.133.35'}
Rating: 0

193.136.172.175 - boromir.ua.pt

name: boromir.ua.pt
ports: {'open': {'1720': {'type': 'tcp', 'state': 'open', 'service': 'h323q931?', 'version': ''}}, 'Filtered': ' 999 filtered tcp ports '}
OS: OpenBSD 4.0
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', 'boromir.ua.pt': '193.136.172.175'}
Rating: 0

193.137.172.2 - bscw.bio.ua.pt

name: bscw.bio.ua.pt
ports: {'open': {'80': {'type': 'tcp', 'state': 'open', 'service': 'http', 'version': 'Apachehttpd2.4.52(OpenSSL/1.1.1mPHP/7.3.33)'}, '443': {'type': 'tcp', 'state': 'open', 'service': 'ssl/http', 'version': 'Apachehttpd2.4.52((Win64)OpenSSL/1.1.1mPHP/7.3.33)'}}, 'Filtered': ' 998 filtered tcp ports '}
OS: Microsoft Windows XP SP3
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', '10.1.0.92': '10.1.0.92', 'assay.bio.ua.pt': '193.137.172.2'}

CVE-2019-13115

cvss: 5.8
severity: Medium
cwe: CWE-190
cvss-vector: AV:N/AC:M/Au:N/C:P/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}
Rating: 5.8

10.55.14.3 - bud-ev2.ua.pt

name: bud-ev2.ua.pt
ports: {'open': {'80': {'type': 'tcp', 'state': 'closed', 'service': 'http', 'version': ''}, '443': {'type': 'tcp', 'state': 'open', 'service': 'ssl/http', 'version': 'Apachehttpd'}, '1720': {'type': 'tcp', 'state': 'open', 'service': 'h323q931?', 'version': ''}}, 'Filtered': ' 997 filtered tcp ports '}
OS:
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', '10.1.0.92': '10.1.0.92', 'fw-vsdc.ua.pt': '193.137.173.236', '10.55.14.3': '10.55.14.3'}

CVE-2001-0131

cvss: 3.3
severity: Low
cwe: CWE-59
cvss-vector: AV:L/AC:M/Au:N/C:N/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'LOCAL'}

CVE-2002-0563

cvss: 5.0
severity: Medium
cwe: CWE-287
cvss-vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2008-1327

cvss: 7.5
severity: High
cwe: CWE-287
cvss-vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2009-0038

cvss: 4.3
severity: Medium
cwe: CWE-79
cvss-vector: AV:N/AC:M/Au:N/C:N/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'NONE', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2010-3449

cvss: 6.8
severity: Medium
cwe: CWE-352
cvss-vector: AV:N/AC:M/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2011-0533

cvss: 4.3
severity: Medium
cwe: CWE-79
cvss-vector: AV:N/AC:M/Au:N/C:N/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'NONE', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2013-0340

cvss: 6.8
severity: Medium
cwe: CWE-611
cvss-vector: AV:N/AC:M/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2014-0085

cvss: 2.1
severity: Low
cwe: CWE-255
cvss-vector: AV:L/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'LOCAL'}

CVE-2014-6271

cvss: 10.0
severity: Critical
cwe: CWE-78
cvss-vector: AV:N/AC:L/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2015-8982

cvss: 6.8
severity: Medium
cwe: CWE-190
cvss-vector: AV:N/AC:M/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2016-1234

cvss: 5.0
severity: Medium
cwe: CWE-119
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2016-2166

cvss: 5.8
severity: Medium
cwe: CWE-200
cvss-vector: AV:N/AC:M/Au:N/C:P/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2016-4462

cvss: 6.5
severity: Medium
cwe: CWE-20
cvss-vector: AV:N/AC:L/Au:S/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'SINGLE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2016-5387

cvss: 5.1
severity: Medium
cwe: CWE-284
cvss-vector: AV:N/AC:H/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'HIGH', 'vector': 'NETWORK'}

CVE-2016-5388

cvss: 5.1
severity: Medium
cwe: CWE-284
cvss-vector: AV:N/AC:H/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'HIGH', 'vector': 'NETWORK'}

CVE-2016-5582

cvss: 9.3
severity: Critical
cwe: CWE-284
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2016-6799

cvss: 5.0
severity: Medium
cwe: CWE-532
cvss-vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2017-15714

cvss: 7.5
severity: High
cwe: CWE-74
cvss-vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2017-17837

cvss: 4.3
severity: Medium
cwe: CWE-79
cvss-vector: AV:N/AC:M/Au:N/C:N/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'NONE', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2018-11786

cvss: 9.0
severity: Critical
cwe: CWE-269
cvss-vector: AV:N/AC:L/Au:S/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'SINGLE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2018-1199

cvss: 5.0
severity: Medium
cwe: CWE-20
cvss-vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2018-1336

cvss: 5.0
severity: Medium
cwe: CWE-835
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2018-16890

cvss: 5.0
severity: Medium
cwe: CWE-125
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2018-8010

cvss: 2.1
severity: Low
cwe: CWE-611
cvss-vector: AV:L/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'LOCAL'}

CVE-2018-8039

cvss: 6.8
severity: Medium
cwe: CWE-755
cvss-vector: AV:N/AC:M/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2019-0224

cvss: 4.3
severity: Medium
cwe: CWE-79
cvss-vector: AV:N/AC:M/Au:N/C:N/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'NONE', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2019-11231

cvss: 5.0
severity: Medium
cwe: CWE-22
cvss-vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-12401

cvss: 5.0
severity: Medium
cwe: CWE-776
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-12405

cvss: 6.8
severity: Medium
cwe: CWE-287
cvss-vector: AV:N/AC:M/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2019-12409

cvss: 7.5
severity: High
cwe: CWE-434
cvss-vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-12418

cvss: 4.4
severity: Medium
cwe: CWE-522
cvss-vector: AV:L/AC:M/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'LOCAL'}

CVE-2019-13012

cvss: 5.0
severity: Medium
cwe: CWE-732
cvss-vector: AV:N/AC:L/Au:N/C:N/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'NONE', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-13050

cvss: 5.0
severity: Medium
cwe: CWE-295
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-13115

cvss: 5.8
severity: Medium
cwe: CWE-190
cvss-vector: AV:N/AC:M/Au:N/C:P/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2019-13565

cvss: 5.0
severity: Medium
cwe: NVD-CWE-noinfo
cvss-vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-16056

cvss: 5.0
severity: Medium
cwe: NVD-CWE-noinfo
cvss-vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-17560

cvss: 6.4
severity: Medium
cwe: CWE-295
cvss-vector: AV:N/AC:L/Au:N/C:P/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-17570

cvss: 7.5
severity: High
cwe: CWE-502
cvss-vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-3822

cvss: 7.5
severity: High
cwe: CWE-787
cvss-vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-9512

cvss: 7.8
severity: High
cwe: CWE-400
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-9514

cvss: 7.8
severity: High
cwe: CWE-770
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-9515

cvss: 7.8
severity: High
cwe: CWE-770
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-9517

cvss: 7.8
severity: High
cwe: CWE-770
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-9518

cvss: 7.8
severity: High
cwe: CWE-770
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-9853

cvss: 6.8
severity: Medium
cwe: CWE-116
cvss-vector: AV:N/AC:M/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2020-13925

cvss: 10.0
severity: Critical
cwe: CWE-78
cvss-vector: AV:N/AC:L/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2020-13926

cvss: 7.5
severity: High
cwe: CWE-89
cvss-vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2020-13932

cvss: 4.3
severity: Medium
cwe: CWE-79
cvss-vector: AV:N/AC:M/Au:N/C:N/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'NONE', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2020-13948

cvss: 6.5
severity: Medium
cwe: NVD-CWE-noinfo
cvss-vector: AV:N/AC:L/Au:S/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'SINGLE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2020-13952

cvss: 5.5
severity: Medium
cwe: NVD-CWE-noinfo
cvss-vector: AV:N/AC:L/Au:S/C:P/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'SINGLE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2020-14621

cvss: 5.0
severity: Medium
cwe: NVD-CWE-noinfo
cvss-vector: AV:N/AC:L/Au:N/C:N/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'NONE', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2020-1752

cvss: 3.7
severity: Low
cwe: CWE-416
cvss-vector: AV:L/AC:H/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'HIGH', 'vector': 'LOCAL'}

CVE-2020-25709

cvss: 5.0
severity: Medium
cwe: CWE-617
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2020-7760

cvss: 5.0
severity: Medium
cwe: CWE-400
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-22696

cvss: 5.0
severity: Medium
cwe: CWE-918
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-23336

cvss: 4.0
severity: Medium
cwe: CWE-444
cvss-vector: AV:N/AC:H/Au:N/C:N/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'HIGH', 'vector': 'NETWORK'}

CVE-2021-23937

cvss: 5.0
severity: Medium
cwe: CWE-20
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-26291

cvss: 6.4
severity: Medium
cwe: CWE-346
cvss-vector: AV:N/AC:L/Au:N/C:P/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-26558

cvss: 5.0
severity: Medium
cwe: CWE-502
cvss-vector: AV:N/AC:L/Au:N/C:N/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'NONE', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-30468

cvss: 5.0
severity: Medium
cwe: CWE-400
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-30638

cvss: 5.0
severity: Medium
cwe: CWE-200
cvss-vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-31522

cvss: 7.5
severity: High
cwe: CWE-470
cvss-vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-32626

cvss: 6.5
severity: Medium
cwe: CWE-787
cvss-vector: AV:N/AC:L/Au:S/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'SINGLE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-36774

cvss: 4.0
severity: Medium
cwe: CWE-668
cvss-vector: AV:N/AC:L/Au:S/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'SINGLE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-37136

cvss: 5.0
severity: Medium
cwe: CWE-400
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-37137

cvss: 5.0
severity: Medium
cwe: CWE-400
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-41571

cvss: 4.0
severity: Medium
cwe: CWE-20
cvss-vector: AV:N/AC:L/Au:S/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'SINGLE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-41616

cvss: 7.5
severity: High
cwe: CWE-502
cvss-vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-43297

cvss: 7.5
severity: High
cwe: CWE-502
cvss-vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-44228

cvss: 9.3
severity: Critical
cwe: CWE-502
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2021-45457

cvss: 5.0
severity: Medium
cwe: CWE-522
cvss-vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-45458

cvss: 5.0
severity: Medium
cwe: CWE-326
cvss-vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2022-22932

cvss: 5.0
severity: Medium
cwe: CWE-22
cvss-vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}
Rating: 10.0

193.136.172.89 - bud-old.ua.pt

name: bud-old.ua.pt
ports: {'open': {'80': {'type': 'tcp', 'state': 'open', 'service': 'http', 'version': 'MicrosoftHTTPAPIhttpd2.0(SSDP/UPnP)'}, '443': {'type': 'tcp', 'state': 'open', 'service': 'ssl/http', 'version': 'MicrosoftHTTPAPIhttpd2.0(SSDP/UPnP)'}, '1720': {'type': 'tcp', 'state': 'open', 'service': 'h323q931?', 'version': ''}}, 'Filtered': ' 997 filtered tcp ports '}
OS: Microsoft Windows Server 2008 or 2008 Beta 3
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', 'scsm.ua.pt': '193.136.172.89'}

CVE-2000-0122

cvss: 5.0
severity: Medium
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2006-6627

cvss: 10.0
severity: Critical
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:L/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2008-1447

cvss: 5.0
severity: Medium
cwe: CWE-331
cvss-vector: AV:N/AC:L/Au:N/C:N/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'NONE', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2009-0087

cvss: 9.3
severity: Critical
cwe: NVD-CWE-noinfo
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2009-0100

cvss: 9.3
severity: Critical
cwe: CWE-399
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2009-0550

cvss: 9.3
severity: Critical
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2009-0557

cvss: 9.3
severity: Critical
cwe: CWE-94
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2009-0560

cvss: 9.3
severity: Critical
cwe: CWE-399
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2009-0561

cvss: 9.3
severity: Critical
cwe: CWE-189
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2009-0563

cvss: 9.3
severity: Critical
cwe: CWE-119
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2009-0565

cvss: 9.3
severity: Critical
cwe: CWE-119
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2009-2499

cvss: 8.5
severity: High
cwe: CWE-94
cvss-vector: AV:N/AC:M/Au:S/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'SINGLE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2010-1900

cvss: 9.3
severity: Critical
cwe: CWE-94
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2010-1901

cvss: 9.3
severity: Critical
cwe: CWE-94
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2010-1902

cvss: 9.3
severity: Critical
cwe: CWE-119
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2015-4950

cvss: 4.0
severity: Medium
cwe: CWE-200
cvss-vector: AV:N/AC:L/Au:S/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'SINGLE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2017-0098

cvss: 2.9
severity: Low
cwe: CWE-20
cvss-vector: AV:A/AC:M/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'ADJACENT_NETWORK'}

CVE-2018-5391

cvss: 7.8
severity: High
cwe: CWE-20
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2020-26233

cvss: 3.6
severity: Low
cwe: CWE-706
cvss-vector: AV:N/AC:H/Au:S/C:P/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'SINGLE', 'complexity': 'HIGH', 'vector': 'NETWORK'}

CVE-2020-35608

cvss: 7.2
severity: High
cwe: CWE-74
cvss-vector: AV:L/AC:L/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'LOCAL'}

CVE-2021-21505

cvss: 10.0
severity: Critical
cwe: CWE-522
cvss-vector: AV:N/AC:L/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-44228

cvss: 9.3
severity: Critical
cwe: CWE-502
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}
Rating: 10.0

192.168.180.82 - cc.voip.ua.pt

name: cc.voip.ua.pt
ports: {'open': {}, 'Filtered': ' 1000 filtered tcp ports '}
OS:
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', '10.1.0.92': '10.1.0.92', 'fw-vsdc.ua.pt': '193.137.173.236', '192.168.180.82': '192.168.180.82'}
Rating: 0

193.136.173.84 - certidao.ua.pt

name: certidao.ua.pt
ports: {'open': {'80': {'type': 'tcp', 'state': 'open', 'service': 'http', 'version': 'MicrosoftIIShttpd8.5'}, '443': {'type': 'tcp', 'state': 'open', 'service': 'ssl/http', 'version': 'MicrosoftIIShttpd8.5'}, '1720': {'type': 'tcp', 'state': 'open', 'service': 'h323q931?', 'version': ''}}, 'Filtered': ' 997 filtered tcp ports '}
OS: Microsoft Windows Server 2008 or 2008 Beta 3
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', 'web-ia.ua.pt': '193.136.173.84'}

CVE-1999-0488

cvss: 7.5
severity: High
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2000-0122

cvss: 5.0
severity: Medium
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2000-0160

cvss: 7.6
severity: High
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:H/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'HIGH', 'vector': 'NETWORK'}

CVE-2000-0256

cvss: 7.5
severity: High
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2000-0544

cvss: 5.0
severity: Medium
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2002-0419

cvss: 5.0
severity: Medium
cwe: CWE-200

cvss-vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2004-0790

cvss: 5.0
severity: Medium
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2004-0928

cvss: 5.0
severity: Medium
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2004-1060

cvss: 5.0
severity: Medium
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2004-2383

cvss: 5.1
severity: Medium
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:H/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'HIGH', 'vector': 'NETWORK'}

CVE-2005-0563

cvss: 4.3
severity: Medium
cwe: CWE-79
cvss-vector: AV:N/AC:M/Au:N/C:N/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'NONE', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2006-3697

cvss: 7.2
severity: High
cwe: CWE-264
cvss-vector: AV:L/AC:L/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'LOCAL'}

CVE-2006-3942

cvss: 7.8
severity: High
cwe: CWE-20

cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2006-5395

cvss: 7.5
severity: High
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2006-6627

cvss: 10.0
severity: Critical
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:L/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2007-0038

cvss: 9.3
severity: Critical
cwe: CWE-119
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2007-1765

cvss: 9.3
severity: Critical
cwe: NVD-CWE-noinfo
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2007-6502

cvss: 5.5
severity: Medium
cwe: CWE-200
cvss-vector: AV:N/AC:L/Au:S/C:P/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'SINGLE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2008-0085

cvss: 5.0
severity: Medium
cwe: CWE-200
cvss-vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2008-0107

cvss: 9.0
severity: Critical
cwe: CWE-189

cvss-vector: AV:N/AC:L/Au:S/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'SINGLE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2008-1447

cvss: 5.0
severity: Medium
cwe: CWE-331
cvss-vector: AV:N/AC:L/Au:N/C:N/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'NONE', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2008-3243

cvss: 4.3
severity: Medium
cwe: CWE-20
cvss-vector: AV:N/AC:M/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2009-0087

cvss: 9.3
severity: Critical
cwe: NVD-CWE-noinfo
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2009-0100

cvss: 9.3
severity: Critical
cwe: CWE-399
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2009-0550

cvss: 9.3
severity: Critical
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2009-0557

cvss: 9.3
severity: Critical
cwe: CWE-94
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2009-0560

cvss: 9.3
severity: Critical
cwe: CWE-399

cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2009-0561

cvss: 9.3
severity: Critical
cwe: CWE-189
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2009-0563

cvss: 9.3
severity: Critical
cwe: CWE-119
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2009-0565

cvss: 9.3
severity: Critical
cwe: CWE-119
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2009-1134

cvss: 9.3
severity: Critical
cwe: CWE-94
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2009-2499

cvss: 8.5
severity: High
cwe: CWE-94
cvss-vector: AV:N/AC:M/Au:S/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'SINGLE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2010-1263

cvss: 9.3
severity: Critical
cwe: CWE-94
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2010-1425

cvss: 5.0
severity: Medium
cwe: NVD-CWE-Other

cvss-vector: AV:N/AC:L/Au:N/C:N/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'NONE', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2010-1900

cvss: 9.3
severity: Critical
cwe: CWE-94
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2010-1901

cvss: 9.3
severity: Critical
cwe: CWE-94
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2010-1902

cvss: 9.3
severity: Critical
cwe: CWE-119
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2012-1854

cvss: 6.9
severity: Medium
cwe: NVD-CWE-Other
cvss-vector: AV:L/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'LOCAL'}

CVE-2015-4950

cvss: 4.0
severity: Medium
cwe: CWE-200
cvss-vector: AV:N/AC:L/Au:S/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'SINGLE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2015-6557

cvss: 2.1
severity: Low
cwe: CWE-200
cvss-vector: AV:L/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'LOCAL'}

CVE-2015-7404

cvss: 1.9
severity: Low
cwe: CWE-200

cvss-vector: AV:L/AC:M/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'LOCAL'}

CVE-2017-0098

cvss: 2.9
severity: Low
cwe: CWE-20
cvss-vector: AV:A/AC:M/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'ADJACENT_NETWORK'}

CVE-2018-5282

cvss: 7.2
severity: High
cwe: CWE-787
cvss-vector: AV:L/AC:L/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'LOCAL'}

CVE-2018-5391

cvss: 7.8
severity: High
cwe: CWE-20
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-1000

cvss: 3.5
severity: Low
cwe: CWE-269
cvss-vector: AV:N/AC:M/Au:S/C:N/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'NONE', 'integrity': 'PARTIAL'}
access: {'authentication': 'SINGLE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2019-16863

cvss: 4.3
severity: Medium
cwe: CWE-327
cvss-vector: AV:N/AC:M/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2020-1296

cvss: 2.1
severity: Low
cwe: CWE-200
cvss-vector: AV:L/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'LOCAL'}

CVE-2020-1459

cvss: 2.1
severity: Low
cwe: CWE-200

cvss-vector: AV:L/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'LOCAL'}

CVE-2020-26233

cvss: 3.6
severity: Low
cwe: CWE-706
cvss-vector: AV:N/AC:H/Au:S/C:P/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'SINGLE', 'complexity': 'HIGH', 'vector': 'NETWORK'}

CVE-2020-35608

cvss: 7.2
severity: High
cwe: CWE-74
cvss-vector: AV:L/AC:L/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'LOCAL'}

CVE-2021-21505

cvss: 10.0
severity: Critical
cwe: CWE-522
cvss-vector: AV:N/AC:L/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-38505

cvss: 4.3
severity: Medium
cwe: CWE-668
cvss-vector: AV:N/AC:M/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2021-44228

cvss: 9.3
severity: Critical
cwe: CWE-502
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}
Rating: 10.0

192.168.248.71 - cloud4ies-piloto.ua.pt

name: cloud4ies-piloto.ua.pt
ports: {'open': {}, 'Filtered': ' 1000 filtered tcp ports '}
OS:
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', '10.1.0.92': '10.1.0.92', '192.168.248.71': '192.168.248.71'}
Rating: 0

193.136.175.13 - code.ua.pt

name: code.ua.pt
ports: {'open': {'80': {'type': 'tcp', 'state': 'open', 'service': 'http', 'version': 'Apachehttpd2.2.22((Debian))'}, '443': {'type': 'tcp', 'state': 'open', 'service': 'ssl/http', 'version': 'Thinhttpd'}}, 'Filtered': ' 998 filtered tcp ports '}
OS:

Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', '10.1.0.92': '10.1.0.92', 'code.ua.pt': '193.136.175.13'}

CVE-2008-1327

cvss: 7.5
severity: High
cwe: CWE-287
cvss-vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2013-0340

cvss: 6.8
severity: Medium
cwe: CWE-611
cvss-vector: AV:N/AC:M/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2015-8982

cvss: 6.8
severity: Medium
cwe: CWE-190
cvss-vector: AV:N/AC:M/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2016-1234

cvss: 5.0
severity: Medium
cwe: CWE-119
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2016-5387

cvss: 5.1
severity: Medium
cwe: CWE-284
cvss-vector: AV:N/AC:H/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'HIGH', 'vector': 'NETWORK'}

CVE-2016-5388

cvss: 5.1
severity: Medium
cwe: CWE-284
cvss-vector: AV:N/AC:H/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'HIGH', 'vector': 'NETWORK'}

CVE-2016-5582

cvss: 9.3
severity: Critical
cwe: CWE-284
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}

access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2017-17837

cvss: 4.3
severity: Medium
cwe: CWE-79
cvss-vector: AV:N/AC:M/Au:N/C:N/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'NONE', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2018-1336

cvss: 5.0
severity: Medium
cwe: CWE-835
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2018-8010

cvss: 2.1
severity: Low
cwe: CWE-611
cvss-vector: AV:L/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'LOCAL'}

CVE-2018-8039

cvss: 6.8
severity: Medium
cwe: CWE-755
cvss-vector: AV:N/AC:M/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2019-12405

cvss: 6.8
severity: Medium
cwe: CWE-287
cvss-vector: AV:N/AC:M/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2019-12418

cvss: 4.4
severity: Medium
cwe: CWE-522
cvss-vector: AV:L/AC:M/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'LOCAL'}

CVE-2019-13012

cvss: 5.0
severity: Medium
cwe: CWE-732
cvss-vector: AV:N/AC:L/Au:N/C:N/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'NONE', 'integrity': 'PARTIAL'}

access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-13050

cvss: 5.0
severity: Medium
cwe: CWE-295
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-13115

cvss: 5.8
severity: Medium
cwe: CWE-190
cvss-vector: AV:N/AC:M/Au:N/C:P/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2019-13565

cvss: 5.0
severity: Medium
cwe: NVD-CWE-noinfo
cvss-vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-16056

cvss: 5.0
severity: Medium
cwe: NVD-CWE-noinfo
cvss-vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-17570

cvss: 7.5
severity: High
cwe: CWE-502
cvss-vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-9512

cvss: 7.8
severity: High
cwe: CWE-400
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-9514

cvss: 7.8
severity: High
cwe: CWE-770
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'NONE', 'integrity': 'NONE'}

access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-9518

cvss: 7.8
severity: High
cwe: CWE-770
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-9853

cvss: 6.8
severity: Medium
cwe: CWE-116
cvss-vector: AV:N/AC:M/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2020-13925

cvss: 10.0
severity: Critical
cwe: CWE-78
cvss-vector: AV:N/AC:L/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2020-13926

cvss: 7.5
severity: High
cwe: CWE-89
cvss-vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2020-13932

cvss: 4.3
severity: Medium
cwe: CWE-79
cvss-vector: AV:N/AC:M/Au:N/C:N/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'NONE', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2020-13948

cvss: 6.5
severity: Medium
cwe: NVD-CWE-noinfo
cvss-vector: AV:N/AC:L/Au:S/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'SINGLE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2020-14621

cvss: 5.0
severity: Medium
cwe: NVD-CWE-noinfo
cvss-vector: AV:N/AC:L/Au:N/C:N/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'NONE', 'integrity': 'PARTIAL'}

access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2020-1752

cvss: 3.7
severity: Low
cwe: CWE-416
cvss-vector: AV:L/AC:H/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'HIGH', 'vector': 'LOCAL'}

CVE-2020-25709

cvss: 5.0
severity: Medium
cwe: CWE-617
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-22696

cvss: 5.0
severity: Medium
cwe: CWE-918
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-23336

cvss: 4.0
severity: Medium
cwe: CWE-444
cvss-vector: AV:N/AC:H/Au:N/C:N/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'HIGH', 'vector': 'NETWORK'}

CVE-2021-26291

cvss: 6.4
severity: Medium
cwe: CWE-346
cvss-vector: AV:N/AC:L/Au:N/C:P/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-26558

cvss: 5.0
severity: Medium
cwe: CWE-502
cvss-vector: AV:N/AC:L/Au:N/C:N/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'NONE', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-30468

cvss: 5.0
severity: Medium
cwe: CWE-400
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}

access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-30638

cvss: 5.0
severity: Medium
cwe: CWE-200
cvss-vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-36774

cvss: 4.0
severity: Medium
cwe: CWE-668
cvss-vector: AV:N/AC:L/Au:S/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'SINGLE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-37136

cvss: 5.0
severity: Medium
cwe: CWE-400
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-37137

cvss: 5.0
severity: Medium
cwe: CWE-400
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}
Rating: 10.0

193.137.173.211 - ctf-metared-2021.ua.pt

name: ctf-metared-2021.ua.pt
ports: {'open': {}, 'Filtered': ' 1000 filtered tcp ports '}
OS:
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', '10.1.0.92': '10.1.0.92', 'gt1-vrfinternet-r.core.ua.pt': '193.137.173.244', '193.137.173.211': '193.137.173.211'}
Rating: 0

193.137.172.47 - dcspt-drivitup.ua.pt

name: dcspt-drivitup.ua.pt
ports: {'open': {'80': {'type': 'tcp', 'state': 'open', 'service': 'http', 'version': 'nginx'}, '443': {'type': 'tcp', 'state': 'open', 'service': 'ssl/http', 'version': 'nginx'}}, 'Filtered': ' 998 filtered tcp ports '}
OS: Linux 4.15 - 5.6
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', '10.1.0.92': '10.1.0.92', 'dcspt-drivitup.ua.pt': '193.137.172.47'}
Rating: 0

192.168.68.162 - dcspt-lab.ua.pt

name: dcspt-lab.ua.pt
ports: {'open': {}, 'Filtered': ' 1000 filtered tcp ports '}
OS:
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', '10.1.0.92': '10.1.0.92', 'dcspt-lab.ua.pt': '192.168.68.162'}
Rating: 0

193.136.172.173 - denethor.ua.pt

name: denethor.ua.pt
ports: {'open': {'1720': {'type': 'tcp', 'state': 'open', 'service': 'h323q931?', 'version': ''}}, 'Filtered': ' 999 filtered tcp ports '}
OS: OpenBSD 4.0
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', 'denethor.ua.pt': '193.136.172.173'}
Rating: 0

193.136.175.32 - deti-labqar.ua.pt

name: deti-labqar.ua.pt
ports: {'open': {'80': {'type': 'tcp', 'state': 'closed', 'service': 'http', 'version': ''}, '443': {'type': 'tcp', 'state': 'open', 'service': 'ssl/http', 'version': 'nginx1.19.0'}}, 'Filtered': ' 998 filtered tcp ports '}
OS: Linux 2.6.32
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', '10.1.0.92': '10.1.0.92', 'deti-labqar.ua.pt': '193.136.175.32'}
Rating: 0

192.168.160.106 - deti-valormar-update.web.ua.pt

name: deti-valormar-update.web.ua.pt
ports: {'open': {}, 'Filtered': ' 1000 filtered tcp ports '}
OS:
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', '10.1.0.92': '10.1.0.92', '10.1.0.42': '10.1.0.42', '192.168.160.106': '192.168.160.106'}
Rating: 0

192.168.160.118 - deti-valormar.web.ua.pt

name: deti-valormar.web.ua.pt
ports: {'open': {}, 'Filtered': ' 1000 filtered tcp ports '}
OS:
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', '10.1.0.92': '10.1.0.92', '10.1.0.42': '10.1.0.42', '192.168.160.118': '192.168.160.118'}
Rating: 0

193.137.172.95 - dmat-cocalc.ua.pt

name: dmat-cocalc.ua.pt
ports: {'open': {'80': {'type': 'tcp', 'state': 'closed', 'service': 'http', 'version': ''}, '443': {'type': 'tcp', 'state': 'open', 'service': 'ssl/https', 'version': 'nginx/1.18.0(Ubuntu)'}}, 'Filtered': ' 998 filtered tcp ports '}
OS: Linux 2.6.32
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', '10.1.0.92': '10.1.0.92', 'dmat-cocalc.ua.pt': '193.137.172.95'}
Rating: 0

192.92.133.27 - docges-preview.ua.pt

name: docges-preview.ua.pt
ports: {'open': {'80': {'type': 'tcp', 'state': 'open', 'service': 'http', 'version': 'Apachehttpd2.4.6((CentOS)OpenSSL/1.0.2k-fips)'}, '443': {'type': 'tcp', 'state': 'open', 'service': 'ssl/http', 'version': 'Apachehttpd2.4.6((CentOS)OpenSSL/1.0.2k-fips)'}, '1720': {'type': 'tcp', 'state': 'open', 'service': 'h323q931?', 'version': ''}}, 'Filtered': ' 997 filtered tcp ports '}
OS:
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', '10.1.0.92': '10.1.0.92', 'fw-vsdc.ua.pt': '193.137.173.236', 'docges.dev.ua.pt': '192.92.133.27'}

CVE-2019-13115

cvss: 5.8
severity: Medium
cwe: CWE-190
cvss-vector: AV:N/AC:M/Au:N/C:P/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}
Rating: 5.8

193.136.172.103 - docges.ua.pt

name: docges.ua.pt
ports: {'open': {'80': {'type': 'tcp', 'state': 'open', 'service': 'http', 'version': 'Apachehttpd2.4.6((CentOS)OpenSSL/1.0.1e-fips)'}, '443': {'type': 'tcp', 'state': 'open', 'service': 'ssl/http', 'version': 'Apachehttpd2.4.6((CentOS)OpenSSL/1.0.1e-fips)'}, '1720': {'type': 'tcp', 'state': 'open', 'service': 'h323q931?', 'version': ''}}, 'Filtered': ' 997 filtered tcp ports '}

OS:
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', 'glassfish4.ua.pt': '193.136.172.103'}

CVE-2019-13115

cvss: 5.8
severity: Medium
cwe: CWE-190
cvss-vector: AV:N/AC:M/Au:N/C:P/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}
Rating: 5.8

193.136.172.185 - docker1.ua.pt

name: docker1.ua.pt
ports: {'open': {'1720': {'type': 'tcp', 'state': 'open', 'service': 'h323q931?', 'version': ''}}, 'Filtered': ' 999 filtered tcp ports '}
OS: OpenBSD 4.3
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', 'docker1.ua.pt': '193.136.172.185'}
Rating: 0

192.92.133.50 - docker2.dev.ua.pt

name: docker2.dev.ua.pt
ports: {'open': {'1720': {'type': 'tcp', 'state': 'open', 'service': 'h323q931?', 'version': ''}}, 'Filtered': ' 999 filtered tcp ports '}
OS: OpenBSD 4.0
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', 'docker2.staging.ua.pt': '192.92.133.50'}
Rating: 0

193.136.172.186 - docker2.ua.pt

name: docker2.ua.pt
ports: {'open': {'1720': {'type': 'tcp', 'state': 'open', 'service': 'h323q931?', 'version': ''}}, 'Filtered': ' 999 filtered tcp ports '}
OS: OpenBSD 4.0
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', 'docker2.ua.pt': '193.136.172.186'}
Rating: 0

192.92.133.51 - docker3.dev.ua.pt

name: docker3.dev.ua.pt
ports: {'open': {'1720': {'type': 'tcp', 'state': 'open', 'service': 'h323q931?', 'version': ''}}, 'Filtered': ' 999 filtered tcp ports '}
OS: OpenBSD 4.0
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', 'docker3.staging.ua.pt': '192.92.133.51'}
Rating: 0

192.92.133.11 - dspace.dev.ua.pt

name: dspace.dev.ua.pt
ports: {'open': {'1720': {'type': 'tcp', 'state': 'open', 'service': 'h323q931?', 'version': ''}}, 'Filtered': ' 999 filtered tcp ports '}
OS: OpenBSD 4.0
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', 'dspace.dev.ua.pt': '192.92.133.11'}
Rating: 0

193.136.173.12 - ecuidhamus.web.ua.pt

name: ecuidhamus.web.ua.pt
ports: {'open': {'80': {'type': 'tcp', 'state': 'open', 'service': 'http', 'version': 'ProtectedbyCOMODOWAFmod_perl/2.0.11Perl/v5.16.3'}, '443': {'type': 'tcp', 'state': 'open', 'service': 'ssl/https', 'version': 'ProtectedbyCOMODOWAFmod_perl/2.0.11Perl/v5.16.3'}, '1720': {'type': 'tcp', 'state': 'open', 'service': 'h323q931?', 'version': ''}}, 'Filtered': ' 997 filtered tcp ports '}
OS:
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', '10.1.0.92': '10.1.0.92', 'fw-vsdc.ua.pt': '193.137.173.236', 'web-lha.ua.pt': '193.136.173.12'}
Rating: 0

193.137.172.73 - ehealthresp-api.web.ua.pt

name: ehealthresp-api.web.ua.pt
ports: {'open': {'80': {'type': 'tcp', 'state': 'open', 'service': 'http', 'version': 'nginx1.21.1'}, '443': {'type': 'tcp', 'state': 'open', 'service': 'ssl/http', 'version': 'nginx1.21.1'}},

'Filtered': ' 998 filtered tcp ports '}
OS: Linux 4.15 - 5.6
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', '10.1.0.92': '10.1.0.92', 'essua-ehealthresp.ua.pt': '193.137.172.73'}
Rating: 0

193.136.173.93 - elearning-201718.ua.pt

name: elearning-201718.ua.pt
ports: {'open': {'1720': {'type': 'tcp', 'state': 'open', 'service': 'h323q931?', 'version': ''}}, 'Filtered': ' 999 filtered tcp ports '}
OS: OpenBSD 4.0
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', 'moodle3.ua.pt': '193.136.173.93'}
Rating: 0

193.136.173.62 - elearning-202122.ua.pt

name: elearning-202122.ua.pt
ports: {'open': {'1720': {'type': 'tcp', 'state': 'open', 'service': 'h323q931?', 'version': ''}}, 'Filtered': ' 999 filtered tcp ports '}
OS: OpenBSD 4.0
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', 'moodle3-1.ua.pt': '193.136.173.62'}
Rating: 0

193.136.173.95 - elearning-projetos.ua.pt

name: elearning-projetos.ua.pt
ports: {'open': {'80': {'type': 'tcp', 'state': 'open', 'service': 'http', 'version': 'Apachehttpd'}, '443': {'type': 'tcp', 'state': 'open', 'service': 'ssl/http', 'version': 'Apachehttpd'}, '1720': {'type': 'tcp', 'state': 'open', 'service': 'h323q931?', 'version': ''}}, 'Filtered': ' 997 filtered tcp ports '}
OS:
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', '10.1.0.92': '10.1.0.92', 'fw-vsdc.ua.pt': '193.137.173.236', 'elearningvip.ua.pt': '193.136.173.95'}

CVE-2001-0131

cvss: 3.3
severity: Low
cwe: CWE-59
cvss-vector: AV:L/AC:M/Au:N/C:N/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'LOCAL'}

CVE-2002-0563

cvss: 5.0
severity: Medium
cwe: CWE-287
cvss-vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2008-1327

cvss: 7.5
severity: High
cwe: CWE-287
cvss-vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2009-0038

cvss: 4.3
severity: Medium
cwe: CWE-79
cvss-vector: AV:N/AC:M/Au:N/C:N/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'NONE', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2010-3449

cvss: 6.8
severity: Medium
cwe: CWE-352
cvss-vector: AV:N/AC:M/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2011-0533

cvss: 4.3
severity: Medium
cwe: CWE-79
cvss-vector: AV:N/AC:M/Au:N/C:N/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'NONE', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2013-0340

cvss: 6.8
severity: Medium
cwe: CWE-611
cvss-vector: AV:N/AC:M/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2014-0085

cvss: 2.1
severity: Low
cwe: CWE-255
cvss-vector: AV:L/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'LOCAL'}

CVE-2014-6271

cvss: 10.0
severity: Critical
cwe: CWE-78
cvss-vector: AV:N/AC:L/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2015-8982

cvss: 6.8
severity: Medium
cwe: CWE-190
cvss-vector: AV:N/AC:M/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2016-1234

cvss: 5.0
severity: Medium
cwe: CWE-119
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2016-2166

cvss: 5.8
severity: Medium
cwe: CWE-200
cvss-vector: AV:N/AC:M/Au:N/C:P/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2016-4462

cvss: 6.5
severity: Medium
cwe: CWE-20
cvss-vector: AV:N/AC:L/Au:S/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'SINGLE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2016-5387

cvss: 5.1
severity: Medium
cwe: CWE-284
cvss-vector: AV:N/AC:H/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'HIGH', 'vector': 'NETWORK'}

CVE-2016-5388

cvss: 5.1
severity: Medium
cwe: CWE-284
cvss-vector: AV:N/AC:H/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'HIGH', 'vector': 'NETWORK'}

CVE-2016-5582

cvss: 9.3
severity: Critical
cwe: CWE-284
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2016-6799

cvss: 5.0
severity: Medium
cwe: CWE-532
cvss-vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2017-15714

cvss: 7.5
severity: High
cwe: CWE-74
cvss-vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2017-17837

cvss: 4.3
severity: Medium
cwe: CWE-79
cvss-vector: AV:N/AC:M/Au:N/C:N/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'NONE', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2018-11786

cvss: 9.0
severity: Critical
cwe: CWE-269
cvss-vector: AV:N/AC:L/Au:S/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'SINGLE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2018-1199

cvss: 5.0
severity: Medium
cwe: CWE-20
cvss-vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2018-1336

cvss: 5.0
severity: Medium
cwe: CWE-835
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2018-16890

cvss: 5.0
severity: Medium
cwe: CWE-125
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2018-8010

cvss: 2.1
severity: Low
cwe: CWE-611
cvss-vector: AV:L/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'LOCAL'}

CVE-2018-8039

cvss: 6.8
severity: Medium
cwe: CWE-755
cvss-vector: AV:N/AC:M/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2019-0224

cvss: 4.3
severity: Medium
cwe: CWE-79
cvss-vector: AV:N/AC:M/Au:N/C:N/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'NONE', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2019-11231

cvss: 5.0
severity: Medium
cwe: CWE-22
cvss-vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-12401

cvss: 5.0
severity: Medium
cwe: CWE-776
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-12405

cvss: 6.8
severity: Medium
cwe: CWE-287
cvss-vector: AV:N/AC:M/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2019-12409

cvss: 7.5
severity: High
cwe: CWE-434
cvss-vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-12418

cvss: 4.4
severity: Medium
cwe: CWE-522
cvss-vector: AV:L/AC:M/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'LOCAL'}

CVE-2019-13012

cvss: 5.0
severity: Medium
cwe: CWE-732
cvss-vector: AV:N/AC:L/Au:N/C:N/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'NONE', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-13050

cvss: 5.0
severity: Medium
cwe: CWE-295
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-13115

cvss: 5.8
severity: Medium
cwe: CWE-190
cvss-vector: AV:N/AC:M/Au:N/C:P/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2019-13565

cvss: 5.0
severity: Medium
cwe: NVD-CWE-noinfo
cvss-vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-16056

cvss: 5.0
severity: Medium
cwe: NVD-CWE-noinfo
cvss-vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-17560

cvss: 6.4
severity: Medium
cwe: CWE-295
cvss-vector: AV:N/AC:L/Au:N/C:P/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-17570

cvss: 7.5
severity: High
cwe: CWE-502
cvss-vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-3822

cvss: 7.5
severity: High
cwe: CWE-787
cvss-vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-9512

cvss: 7.8
severity: High
cwe: CWE-400
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-9514

cvss: 7.8
severity: High
cwe: CWE-770
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-9515

cvss: 7.8
severity: High
cwe: CWE-770
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-9517

cvss: 7.8
severity: High
cwe: CWE-770
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-9518

cvss: 7.8
severity: High
cwe: CWE-770
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-9853

cvss: 6.8
severity: Medium
cwe: CWE-116
cvss-vector: AV:N/AC:M/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2020-13925

cvss: 10.0
severity: Critical
cwe: CWE-78
cvss-vector: AV:N/AC:L/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2020-13926

cvss: 7.5
severity: High
cwe: CWE-89
cvss-vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2020-13932

cvss: 4.3
severity: Medium
cwe: CWE-79
cvss-vector: AV:N/AC:M/Au:N/C:N/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'NONE', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2020-13948

cvss: 6.5
severity: Medium
cwe: NVD-CWE-noinfo
cvss-vector: AV:N/AC:L/Au:S/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'SINGLE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2020-13952

cvss: 5.5
severity: Medium
cwe: NVD-CWE-noinfo
cvss-vector: AV:N/AC:L/Au:S/C:P/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'SINGLE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2020-14621

cvss: 5.0
severity: Medium
cwe: NVD-CWE-noinfo
cvss-vector: AV:N/AC:L/Au:N/C:N/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'NONE', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2020-1752

cvss: 3.7
severity: Low
cwe: CWE-416
cvss-vector: AV:L/AC:H/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'HIGH', 'vector': 'LOCAL'}

CVE-2020-25709

cvss: 5.0
severity: Medium
cwe: CWE-617
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2020-7760

cvss: 5.0
severity: Medium
cwe: CWE-400
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-22696

cvss: 5.0
severity: Medium
cwe: CWE-918
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-23336

cvss: 4.0
severity: Medium
cwe: CWE-444
cvss-vector: AV:N/AC:H/Au:N/C:N/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'HIGH', 'vector': 'NETWORK'}

CVE-2021-23937

cvss: 5.0
severity: Medium
cwe: CWE-20
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-26291

cvss: 6.4
severity: Medium
cwe: CWE-346
cvss-vector: AV:N/AC:L/Au:N/C:P/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-26558

cvss: 5.0
severity: Medium
cwe: CWE-502
cvss-vector: AV:N/AC:L/Au:N/C:N/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'NONE', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-30468

cvss: 5.0
severity: Medium
cwe: CWE-400
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-30638

cvss: 5.0
severity: Medium
cwe: CWE-200
cvss-vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-31522

cvss: 7.5
severity: High
cwe: CWE-470
cvss-vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-32626

cvss: 6.5
severity: Medium
cwe: CWE-787
cvss-vector: AV:N/AC:L/Au:S/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'SINGLE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-36774

cvss: 4.0
severity: Medium
cwe: CWE-668
cvss-vector: AV:N/AC:L/Au:S/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'SINGLE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-37136

cvss: 5.0
severity: Medium
cwe: CWE-400
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-37137

cvss: 5.0
severity: Medium
cwe: CWE-400
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-41571

cvss: 4.0
severity: Medium
cwe: CWE-20
cvss-vector: AV:N/AC:L/Au:S/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'SINGLE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-41616

cvss: 7.5
severity: High
cwe: CWE-502
cvss-vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-43297

cvss: 7.5
severity: High
cwe: CWE-502
cvss-vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-44228

cvss: 9.3
severity: Critical
cwe: CWE-502
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2021-45457

cvss: 5.0
severity: Medium
cwe: CWE-522
cvss-vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-45458

cvss: 5.0
severity: Medium
cwe: CWE-326
cvss-vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2022-22932

cvss: 5.0
severity: Medium
cwe: CWE-22
cvss-vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}
Rating: 10.0

192.92.133.4 - elearning.dev.ua.pt

name: elearning.dev.ua.pt
ports: {'open': {'1720': {'type': 'tcp', 'state': 'open', 'service': 'h323q931?', 'version': ''}}, 'Filtered': ' 999 filtered tcp ports '}
OS: OpenBSD 4.0
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', 'moodle33.dev.ua.pt': '192.92.133.4'}
Rating: 0

192.168.160.182 - essua-radiologia.ua.pt

name: essua-radiologia.ua.pt
ports: {'open': {}, 'Filtered': ' 1000 filtered tcp ports '}
OS:
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', '10.1.0.92': '10.1.0.92', '10.1.0.42': '10.1.0.42', 'essua-radiologia.ua.pt': '192.168.160.182'}
Rating: 0

192.168.160.239 - eventos.dev.ua.pt

name: eventos.dev.ua.pt
ports: {'open': {}, 'Filtered': ' 1000 filtered tcp ports '}
OS:
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', '10.1.0.92': '10.1.0.92', '10.1.0.42': '10.1.0.42', 'eventos.dev.ua.pt': '192.168.160.239'}
Rating: 0

193.136.173.7 - exchange.ua.pt

name: exchange.ua.pt
ports: {'open': {'25': {'type': 'tcp', 'state': 'open', 'service': 'smtp', 'version': 'MicrosoftExchangesmtpd'}, '80': {'type': 'tcp', 'state': 'open', 'service': 'http', 'version': 'MicrosoftIIShttpd10.0'}, '135': {'type': 'tcp', 'state': 'closed', 'service': 'msrpc', 'version': ''}, '443': {'type': 'tcp', 'state': 'open', 'service': 'ssl/http', 'version': 'MicrosoftIIShttpd10.0'}, '993': {'type': 'tcp', 'state': 'open', 'service': 'ssl/imap', 'version': ''}, '995': {'type': 'tcp', 'state': 'open', 'service': 'ssl/pop3', 'version': ''}, '1720': {'type': 'tcp', 'state': 'open', 'service': 'h323q931?', 'version': ''}}, 'Filtered': ' 993 filtered tcp ports '}
OS: Microsoft Windows Server 2016
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', '10.1.0.92': '10.1.0.92', 'fw-vsdc.ua.pt': '193.137.173.236', 'exchange.ua.pt': '193.136.173.7'}

CVE-2000-0122

cvss: 5.0
severity: Medium
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2000-0256

cvss: 7.5
severity: High
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2004-2383

cvss: 5.1
severity: Medium
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:H/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'HIGH', 'vector': 'NETWORK'}

CVE-2006-3942

cvss: 7.8
severity: High
cwe: CWE-20
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2006-5395

cvss: 7.5
severity: High
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2006-6627

cvss: 10.0
severity: Critical
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:L/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2007-0038

cvss: 9.3
severity: Critical
cwe: CWE-119
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2010-1425

cvss: 5.0
severity: Medium
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:L/Au:N/C:N/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'NONE', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2015-4950

cvss: 4.0
severity: Medium
cwe: CWE-200
cvss-vector: AV:N/AC:L/Au:S/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'SINGLE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2015-6557

cvss: 2.1
severity: Low
cwe: CWE-200
cvss-vector: AV:L/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'LOCAL'}

CVE-2015-7404

cvss: 1.9
severity: Low
cwe: CWE-200
cvss-vector: AV:L/AC:M/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'LOCAL'}
Rating: 10.0

193.136.172.174 - faramir.ua.pt

name: faramir.ua.pt
ports: {'open': {'1720': {'type': 'tcp', 'state': 'open', 'service': 'h323q931?', 'version': ''}}, 'Filtered': ' 999 filtered tcp ports '}
OS: OpenBSD 4.0
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', 'faramir.ua.pt': '193.136.172.174'}
Rating: 0

192.168.253.216 - fed.demo.ua.pt

name: fed.demo.ua.pt
ports: {'open': {}, 'Filtered': ' 1000 filtered tcp ports '}
OS:
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', '10.1.0.92': '10.1.0.92', 'adfs2012r2-proxy.staging.ua.pt': '192.168.253.216'}
Rating: 0

192.92.133.34 - flow-app.qa.ua.pt

name: flow-app.qa.ua.pt
ports: {'open': {'80': {'type': 'tcp', 'state': 'open', 'service': 'http', 'version': 'nginx1.20.2'}, '443': {'type': 'tcp', 'state': 'open', 'service': 'ssl/http', 'version': 'nginx1.20.2'}, '1720': {'type': 'tcp', 'state': 'open', 'service': 'h323q931?', 'version': ''}}, 'Filtered': ' 997 filtered tcp ports '}
OS:
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', 'ng-vip.dev.ua.pt': '192.92.133.34'}
Rating: 0

193.136.173.58 - flow.ua.pt

name: flow.ua.pt
ports: {'open': {'80': {'type': 'tcp', 'state': 'open', 'service': 'http', 'version': 'nginx1.20.2'}, '443': {'type': 'tcp', 'state': 'open', 'service': 'ssl/http', 'version': 'nginx1.20.2'}, '1720': {'type': 'tcp', 'state': 'open', 'service': 'h323q931?', 'version': ''}}, 'Filtered': ' 997 filtered tcp ports '}
OS:
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', '10.1.0.92': '10.1.0.92', 'fw-vsdc.ua.pt': '193.137.173.236', 'lvs-ng.ua.pt': '193.136.173.58'}
Rating: 0

192.92.133.8 - forms.dev.ua.pt

name: forms.dev.ua.pt
ports: {'open': {'1720': {'type': 'tcp', 'state': 'open', 'service': 'h323q931?', 'version': ''}}, 'Filtered': ' 999 filtered tcp ports '}
OS: OpenBSD 4.0
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', 'pp-web-l.dev.ua.pt': '192.92.133.8'}
Rating: 0

193.136.172.11 - galadriel.ua.pt

name: galadriel.ua.pt
ports: {'open': {'1720': {'type': 'tcp', 'state': 'open', 'service': 'h323q931?', 'version': ''}}, 'Filtered': ' 999 filtered tcp ports '}
OS: OpenBSD 4.0
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', 'galadriel.ua.pt': '193.136.172.11'}
Rating: 0

193.136.172.61 - galera-n1.ua.pt

name: galera-n1.ua.pt
ports: {'open': {'1720': {'type': 'tcp', 'state': 'open', 'service': 'h323q931?', 'version': ''}}, 'Filtered': ' 999 filtered tcp ports '}
OS: OpenBSD 4.0
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', 'galera-n1.ua.pt': '193.136.172.61'}
Rating: 0

193.136.172.62 - galera-n2.ua.pt

name: galera-n2.ua.pt
ports: {'open': {'1720': {'type': 'tcp', 'state': 'open', 'service': 'h323q931?', 'version': ''}}, 'Filtered': ' 999 filtered tcp ports '}
OS: OpenBSD 4.0
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', 'galera-n2.ua.pt': '193.136.172.62'}
Rating: 0

193.136.172.58 - galera2-n1.ua.pt

name: galera2-n1.ua.pt
ports: {'open': {'1720': {'type': 'tcp', 'state': 'open', 'service': 'h323q931?', 'version': ''}}, 'Filtered': ' 999 filtered tcp ports '}
OS: OpenBSD 4.0
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', 'galera2-n1.ua.pt': '193.136.172.58'}
Rating: 0

193.137.172.81 - geo-navsafety.ua.pt

name: geo-navsafety.ua.pt
ports: {'open': {'80': {'type': 'tcp', 'state': 'closed', 'service': 'http', 'version': ''}, '81': {'type': 'tcp', 'state': 'closed', 'service': 'hosts2-ns', 'version': ''}, '443': {'type': 'tcp', 'state': 'closed', 'service': 'https', 'version': ''}}, 'Filtered': ' 997 filtered tcp ports '}
OS:
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', '10.1.0.92': '10.1.0.92', 'geo-navsafety.ua.pt': '193.137.172.81'}
Rating: 0

193.136.173.39 - gest.unave.ua.pt

name: gest.unave.ua.pt
ports: {'open': {'1720': {'type': 'tcp', 'state': 'open', 'service': 'h323q931?', 'version': ''}}, 'Filtered': ' 999 filtered tcp ports '}
OS: OpenBSD 4.0
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', 'gest.unave.ua.pt': '193.136.173.39'}
Rating: 0

193.136.172.137 - girafa.cic.ua.pt

name: girafa.cic.ua.pt
ports: {'open': {'1720': {'type': 'tcp', 'state': 'open', 'service': 'h323q931?', 'version': ''}}, 'Filtered': ' 999 filtered tcp ports '}
OS: OpenBSD 4.0
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', 'aplicacoes.servers.ua.pt': '193.136.172.137'}
Rating: 0

193.136.175.23 - glua.ua.pt

name: glua.ua.pt
ports: {'open': {'21': {'type': 'tcp', 'state': 'open', 'service': 'ftp', 'version': 'vsftpd3.0.2'}, '80': {'type': 'tcp', 'state': 'open', 'service': 'http', 'version': 'nginx1.20.2'}, '443': {'type': 'tcp', 'state': 'open', 'service': 'ssl/http', 'version': 'nginx1.20.2'}, '873': {'type': 'tcp', 'state': 'open', 'service': 'rsync', 'version': '(protocolversion31)'}}, 'Filtered': ' 996 filtered tcp ports '}
OS:
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', '10.1.0.92': '10.1.0.92', 'glua.ieeta.pt': '193.136.175.23'}
Rating: 0

193.137.173.235 - go.ua.pt

name: go.ua.pt
ports: {'open': {'264': {'type': 'tcp', 'state': 'open', 'service': 'fw1-topology', 'version': 'CheckPointFireWall-1Topology'}}, 'Filtered': ' 999 filtered tcp ports '}
OS: Linux 3.10 - 4.11
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', '10.1.0.92': '10.1.0.92', 'fw-vsvpn.ua.pt': '193.137.173.235'}

CVE-2008-5994

cvss: 4.3
severity: Medium
cwe: CWE-79
cvss-vector: AV:N/AC:M/Au:N/C:N/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'NONE', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2013-1359

cvss: 10.0
severity: Critical
cwe: CWE-287
cvss-vector: AV:N/AC:L/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2014-6271

cvss: 10.0
severity: Critical
cwe: CWE-78
cvss-vector: AV:N/AC:L/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2017-9106

cvss: 5.0
severity: Medium
cwe: CWE-119
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2020-15137

cvss: 3.6
severity: Low
cwe: CWE-190
cvss-vector: AV:L/AC:L/Au:N/C:P/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'LOCAL'}

CVE-2020-6021

cvss: 4.4
severity: Medium
cwe: CWE-427
cvss-vector: AV:L/AC:M/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'LOCAL'}

CVE-2021-34405

cvss: 4.9
severity: Medium
cwe: CWE-476
cvss-vector: AV:L/AC:L/Au:N/C:N/I:N/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'LOCAL'}
Rating: 10.0

193.137.172.64 - govcopp-dsslab.ua.pt

name: govcopp-dsslab.ua.pt
ports: {'open': {'80': {'type': 'tcp', 'state': 'closed', 'service': 'http', 'version': ''}, '443': {'type': 'tcp', 'state': 'closed', 'service': 'https', 'version': ''}}, 'Filtered': ' 998 filtered tcp ports '}
OS:
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', '10.1.0.92': '10.1.0.92', 'dcspt-govcopp.ua.pt': '193.137.172.64'}
Rating: 0

192.168.164.130 - gq.sas.ua.pt

name: gq.sas.ua.pt
ports: {'open': {}, 'Filtered': ' 1000 filtered tcp ports '}
OS:
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', '10.1.0.92': '10.1.0.92', 'fw-vsdc.ua.pt': '193.137.173.236', 'sas-srv.ua.pt': '192.168.164.130'}
Rating: 0

193.136.173.103 - identity.ua.pt

name: identity.ua.pt
ports: {'open': {'80': {'type': 'tcp', 'state': 'open', 'service': 'http', 'version': 'Apachehttpd(PHP5.3.3)'}, '443': {'type': 'tcp', 'state': 'open', 'service': 'ssl/http', 'version': 'Apachehttpd(PHP5.3.3)'}, '1720': {'type': 'tcp', 'state': 'open', 'service': 'h323q931?', 'version': ''}}, 'Filtered': ' 997 filtered tcp ports '}
OS:
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', '10.1.0.92': '10.1.0.92', 'fw-vsdc.ua.pt': '193.137.173.236', 'identity.ua.pt': '193.136.173.103'}

CVE-2001-0131

cvss: 3.3
severity: Low
cwe: CWE-59
cvss-vector: AV:L/AC:M/Au:N/C:N/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'LOCAL'}

CVE-2002-0563

cvss: 5.0
severity: Medium
cwe: CWE-287
cvss-vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2008-1327

cvss: 7.5
severity: High
cwe: CWE-287
cvss-vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2009-0038

cvss: 4.3
severity: Medium
cwe: CWE-79
cvss-vector: AV:N/AC:M/Au:N/C:N/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'NONE', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2010-3449

cvss: 6.8
severity: Medium
cwe: CWE-352
cvss-vector: AV:N/AC:M/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2011-0533

cvss: 4.3
severity: Medium
cwe: CWE-79
cvss-vector: AV:N/AC:M/Au:N/C:N/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'NONE', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2013-0340

cvss: 6.8
severity: Medium
cwe: CWE-611
cvss-vector: AV:N/AC:M/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2014-0085

cvss: 2.1
severity: Low
cwe: CWE-255
cvss-vector: AV:L/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'LOCAL'}

CVE-2014-6271

cvss: 10.0
severity: Critical
cwe: CWE-78
cvss-vector: AV:N/AC:L/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2015-8982

cvss: 6.8
severity: Medium
cwe: CWE-190
cvss-vector: AV:N/AC:M/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2016-1234

cvss: 5.0
severity: Medium
cwe: CWE-119
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2016-2166

cvss: 5.8
severity: Medium
cwe: CWE-200
cvss-vector: AV:N/AC:M/Au:N/C:P/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2016-4462

cvss: 6.5
severity: Medium
cwe: CWE-20
cvss-vector: AV:N/AC:L/Au:S/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'SINGLE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2016-5387

cvss: 5.1
severity: Medium
cwe: CWE-284
cvss-vector: AV:N/AC:H/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'HIGH', 'vector': 'NETWORK'}

CVE-2016-5388

cvss: 5.1
severity: Medium
cwe: CWE-284
cvss-vector: AV:N/AC:H/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'HIGH', 'vector': 'NETWORK'}

CVE-2016-5582

cvss: 9.3
severity: Critical
cwe: CWE-284
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2016-6799

cvss: 5.0
severity: Medium
cwe: CWE-532
cvss-vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2017-15714

cvss: 7.5
severity: High
cwe: CWE-74
cvss-vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2017-17837

cvss: 4.3
severity: Medium
cwe: CWE-79
cvss-vector: AV:N/AC:M/Au:N/C:N/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'NONE', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2018-11786

cvss: 9.0
severity: Critical
cwe: CWE-269
cvss-vector: AV:N/AC:L/Au:S/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'SINGLE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2018-1199

cvss: 5.0
severity: Medium
cwe: CWE-20
cvss-vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2018-1336

cvss: 5.0
severity: Medium
cwe: CWE-835
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2018-16890

cvss: 5.0
severity: Medium
cwe: CWE-125
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2018-8010

cvss: 2.1
severity: Low
cwe: CWE-611
cvss-vector: AV:L/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'LOCAL'}

CVE-2018-8039

cvss: 6.8
severity: Medium
cwe: CWE-755
cvss-vector: AV:N/AC:M/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2019-0224

cvss: 4.3
severity: Medium
cwe: CWE-79
cvss-vector: AV:N/AC:M/Au:N/C:N/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'NONE', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2019-11231

cvss: 5.0
severity: Medium
cwe: CWE-22
cvss-vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-12401

cvss: 5.0
severity: Medium
cwe: CWE-776
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-12405

cvss: 6.8
severity: Medium
cwe: CWE-287
cvss-vector: AV:N/AC:M/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2019-12409

cvss: 7.5
severity: High
cwe: CWE-434
cvss-vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-12418

cvss: 4.4
severity: Medium
cwe: CWE-522
cvss-vector: AV:L/AC:M/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'LOCAL'}

CVE-2019-13012

cvss: 5.0
severity: Medium
cwe: CWE-732
cvss-vector: AV:N/AC:L/Au:N/C:N/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'NONE', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-13050

cvss: 5.0
severity: Medium
cwe: CWE-295
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-13115

cvss: 5.8
severity: Medium
cwe: CWE-190
cvss-vector: AV:N/AC:M/Au:N/C:P/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2019-13565

cvss: 5.0
severity: Medium
cwe: NVD-CWE-noinfo
cvss-vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-16056

cvss: 5.0
severity: Medium
cwe: NVD-CWE-noinfo
cvss-vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-17560

cvss: 6.4
severity: Medium
cwe: CWE-295
cvss-vector: AV:N/AC:L/Au:N/C:P/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-17570

cvss: 7.5
severity: High
cwe: CWE-502
cvss-vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-3822

cvss: 7.5
severity: High
cwe: CWE-787
cvss-vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-9512

cvss: 7.8
severity: High
cwe: CWE-400
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-9514

cvss: 7.8
severity: High
cwe: CWE-770
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-9515

cvss: 7.8
severity: High
cwe: CWE-770
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-9517

cvss: 7.8
severity: High
cwe: CWE-770
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-9518

cvss: 7.8
severity: High
cwe: CWE-770
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-9853

cvss: 6.8
severity: Medium
cwe: CWE-116
cvss-vector: AV:N/AC:M/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2020-13925

cvss: 10.0
severity: Critical
cwe: CWE-78
cvss-vector: AV:N/AC:L/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2020-13926

cvss: 7.5
severity: High
cwe: CWE-89
cvss-vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2020-13932

cvss: 4.3
severity: Medium
cwe: CWE-79
cvss-vector: AV:N/AC:M/Au:N/C:N/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'NONE', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2020-13948

cvss: 6.5
severity: Medium
cwe: NVD-CWE-noinfo
cvss-vector: AV:N/AC:L/Au:S/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'SINGLE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2020-13952

cvss: 5.5
severity: Medium
cwe: NVD-CWE-noinfo
cvss-vector: AV:N/AC:L/Au:S/C:P/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'SINGLE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2020-14621

cvss: 5.0
severity: Medium
cwe: NVD-CWE-noinfo
cvss-vector: AV:N/AC:L/Au:N/C:N/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'NONE', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2020-1752

cvss: 3.7
severity: Low
cwe: CWE-416
cvss-vector: AV:L/AC:H/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'HIGH', 'vector': 'LOCAL'}

CVE-2020-25709

cvss: 5.0
severity: Medium
cwe: CWE-617
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2020-7760

cvss: 5.0
severity: Medium
cwe: CWE-400
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-22696

cvss: 5.0
severity: Medium
cwe: CWE-918
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-23336

cvss: 4.0
severity: Medium
cwe: CWE-444
cvss-vector: AV:N/AC:H/Au:N/C:N/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'HIGH', 'vector': 'NETWORK'}

CVE-2021-23937

cvss: 5.0
severity: Medium
cwe: CWE-20
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-26291

cvss: 6.4
severity: Medium
cwe: CWE-346
cvss-vector: AV:N/AC:L/Au:N/C:P/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-26558

cvss: 5.0
severity: Medium
cwe: CWE-502
cvss-vector: AV:N/AC:L/Au:N/C:N/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'NONE', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-30468

cvss: 5.0
severity: Medium
cwe: CWE-400
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-30638

cvss: 5.0
severity: Medium
cwe: CWE-200
cvss-vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-31522

cvss: 7.5
severity: High
cwe: CWE-470
cvss-vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-32626

cvss: 6.5
severity: Medium
cwe: CWE-787
cvss-vector: AV:N/AC:L/Au:S/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'SINGLE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-36774

cvss: 4.0
severity: Medium
cwe: CWE-668
cvss-vector: AV:N/AC:L/Au:S/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'SINGLE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-37136

cvss: 5.0
severity: Medium
cwe: CWE-400
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-37137

cvss: 5.0
severity: Medium
cwe: CWE-400
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-41571

cvss: 4.0
severity: Medium
cwe: CWE-20
cvss-vector: AV:N/AC:L/Au:S/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'SINGLE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-41616

cvss: 7.5
severity: High
cwe: CWE-502
cvss-vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-43297

cvss: 7.5
severity: High
cwe: CWE-502
cvss-vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-44228

cvss: 9.3
severity: Critical
cwe: CWE-502
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2021-45457

cvss: 5.0
severity: Medium
cwe: CWE-522
cvss-vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-45458

cvss: 5.0
severity: Medium
cwe: CWE-326
cvss-vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2022-22932

cvss: 5.0
severity: Medium
cwe: CWE-22
cvss-vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}
Rating: 10.0

193.136.173.100 - idp.ua.pt

name: idp.ua.pt
ports: {'open': {'443': {'type': 'tcp', 'state': 'open', 'service': 'ssl/http', 'version': 'MicrosoftHTTPAPIhttpd2.0(SSDP/UPnP)'}, '1720': {'type': 'tcp', 'state': 'open', 'service': 'h323q931?', 'version': ''}}, 'Filtered': ' 998 filtered tcp ports '}
OS: Microsoft Windows Server 2016
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', 'idp.ua.pt': '193.136.173.100'}

CVE-2000-0122

cvss: 5.0
severity: Medium
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2006-6627

cvss: 10.0
severity: Critical
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:L/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2008-1447

cvss: 5.0
severity: Medium
cwe: CWE-331
cvss-vector: AV:N/AC:L/Au:N/C:N/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'NONE', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2009-0087

cvss: 9.3
severity: Critical
cwe: NVD-CWE-noinfo
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2009-0100

cvss: 9.3
severity: Critical
cwe: CWE-399
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2009-0550

cvss: 9.3
severity: Critical
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2009-0557

cvss: 9.3
severity: Critical
cwe: CWE-94
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2009-0560

cvss: 9.3
severity: Critical
cwe: CWE-399
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2009-0561

cvss: 9.3
severity: Critical
cwe: CWE-189
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2009-0563

cvss: 9.3
severity: Critical
cwe: CWE-119
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2009-0565

cvss: 9.3
severity: Critical
cwe: CWE-119
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2009-2499

cvss: 8.5
severity: High
cwe: CWE-94
cvss-vector: AV:N/AC:M/Au:S/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'SINGLE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2010-1900

cvss: 9.3
severity: Critical
cwe: CWE-94
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2010-1901

cvss: 9.3
severity: Critical
cwe: CWE-94
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2010-1902

cvss: 9.3
severity: Critical
cwe: CWE-119
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2015-4950

cvss: 4.0
severity: Medium
cwe: CWE-200
cvss-vector: AV:N/AC:L/Au:S/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'SINGLE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2017-0098

cvss: 2.9
severity: Low
cwe: CWE-20
cvss-vector: AV:A/AC:M/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'ADJACENT_NETWORK'}

CVE-2018-5391

cvss: 7.8
severity: High
cwe: CWE-20
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2020-26233

cvss: 3.6
severity: Low
cwe: CWE-706
cvss-vector: AV:N/AC:H/Au:S/C:P/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'SINGLE', 'complexity': 'HIGH', 'vector': 'NETWORK'}

CVE-2020-35608

cvss: 7.2
severity: High
cwe: CWE-74
cvss-vector: AV:L/AC:L/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'LOCAL'}

CVE-2021-21505

cvss: 10.0
severity: Critical
cwe: CWE-522
cvss-vector: AV:N/AC:L/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-44228

cvss: 9.3
severity: Critical
cwe: CWE-502
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}
Rating: 10.0

193.136.175.4 - ieeta-cloudpt.web.ua.pt

name: ieeta-cloudpt.web.ua.pt
ports: {'open': {'80': {'type': 'tcp', 'state': 'open', 'service': 'http', 'version': 'nginx1.19.10'}, '443': {'type': 'tcp', 'state': 'open', 'service': 'ssl/http', 'version': 'nginx1.19.10'}, '8081': {'type': 'tcp', 'state': 'closed', 'service': 'blackice-icecap', 'version': ''}}, 'Filtered': ' 997 filtered tcp ports '}
OS: Linux 2.6.32
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', '10.1.0.92': '10.1.0.92', 'portal.ieeta.pt': '193.136.175.4'}
Rating: 0

40.84.227.188 - imc.web.ua.pt

name: imc.web.ua.pt
ports: {'open': {'5060': {'type': 'tcp', 'state': 'open', 'service': 'sip?', 'version': ''}}, 'Filtered': ' 999 filtered tcp ports '}
OS: OpenBSD 4.0
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', '40.84.227.188': '40.84.227.188'}
Rating: 0

193.137.172.20 - ims.mec.ua.pt

name: ims.mec.ua.pt
ports: {'open': {'80': {'type': 'tcp', 'state': 'open', 'service': 'http', 'version': 'MicrosoftIIShttpd10.0'}, '443': {'type': 'tcp', 'state': 'open', 'service': 'ssl/http', 'version': 'MicrosoftHTTPAPIhttpd2.0(SSDP/UPnP)'}}, 'Filtered': ' 998 filtered tcp ports '}
OS: Microsoft Windows XP SP3
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', '10.1.0.92': '10.1.0.92', 'ims.mec.ua.pt': '193.137.172.20'}

CVE-2021-38505

cvss: 4.3
severity: Medium
cwe: CWE-668
cvss-vector: AV:N/AC:M/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}
Rating: 4.3

193.137.172.71 - locallproject.web.ua.pt

name: locallproject.web.ua.pt
ports: {'open': {'80': {'type': 'tcp', 'state': 'open', 'service': 'http', 'version': 'Apachehttpd2.4.29'}, '443': {'type': 'tcp', 'state': 'open', 'service': 'ssl/http', 'version': 'Apachehttpd2.4.29((Ubuntu))'}}, 'Filtered': ' 998 filtered tcp ports '}
OS: Linux 5.0 - 5.3
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', '10.1.0.92': '10.1.0.92', 'dep-oesc.ua.pt': '193.137.172.71'}

CVE-2019-13115

cvss: 5.8
severity: Medium
cwe: CWE-190
cvss-vector: AV:N/AC:M/Au:N/C:P/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}
Rating: 5.8

192.168.253.7 - logs.staging.ua.pt

name: logs.staging.ua.pt
ports: {'open': {}, 'Filtered': ' 1000 filtered tcp ports '}
OS:
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', '10.1.0.92': '10.1.0.92', 'k8s-staging-lvs.staging.ua.pt': '192.168.253.7'}
Rating: 0

192.168.253.200 - mail.demo.ua.pt

name: mail.demo.ua.pt
ports: {'open': {}, 'Filtered': ' 1000 filtered tcp ports '}
OS:
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', '10.1.0.92': '10.1.0.92', 'mail.staging.ua.pt': '192.168.253.200'}
Rating: 0

193.137.172.94 - megua.ua.pt

name: megua.ua.pt
ports: {'open': {'80': {'type': 'tcp', 'state': 'open', 'service': 'http', 'version': 'Apachehttpd2.4.29((Ubuntu))'}, '443': {'type': 'tcp', 'state': 'closed', 'service': 'https', 'version': ''}}, 'Filtered': ' 998 filtered tcp ports '}
OS: Linux 2.6.32
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', '10.1.0.92': '10.1.0.92', 'megua.ua.pt': '193.137.172.94'}

CVE-2019-13115

cvss: 5.8
severity: Medium
cwe: CWE-190
cvss-vector: AV:N/AC:M/Au:N/C:P/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}
Rating: 5.8

193.137.172.67 - mixmyvisit.web.ua.pt

name: mixmyvisit.web.ua.pt
ports: {'open': {'80': {'type': 'tcp', 'state': 'open', 'service': 'http', 'version': 'nginx1.14.0(Ubuntu)'}, '443': {'type': 'tcp', 'state': 'open', 'service': 'ssl/http', 'version': 'nginx1.14.0(Ubuntu)'}, '3333': {'type': 'tcp', 'state': 'closed', 'service': 'dec-notes', 'version': ''}, '6001': {'type': 'tcp', 'state': 'closed', 'service': 'X11:1', 'version': ''}}, 'Filtered': ' 996 filtered tcp ports '}
OS: Linux 2.6.32 or 3.10
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', '10.1.0.92': '10.1.0.92', 'deca-mixmyvisit.ua.pt': '193.137.172.67'}
Rating: 0

193.136.173.2 - mx01.ua.pt

name: mx01.ua.pt
ports: {'open': {'25': {'type': 'tcp', 'state': 'open', 'service': 'smtp', 'version': 'MicrosoftExchangesmtpd'}, '1720': {'type': 'tcp', 'state': 'open', 'service': 'h323q931?', 'version': ''}}, 'Filtered': ' 998 filtered tcp ports '}
OS:
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', '10.1.0.92': '10.1.0.92', 'fw-vsdc.ua.pt': '193.137.173.236', 'mx01.ua.pt': '193.136.173.2'}

CVE-2000-0122

cvss: 5.0
severity: Medium
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2000-0256

cvss: 7.5
severity: High
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2004-2383

cvss: 5.1
severity: Medium
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:H/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'HIGH', 'vector': 'NETWORK'}

CVE-2006-3942

cvss: 7.8
severity: High
cwe: CWE-20
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2006-5395

cvss: 7.5
severity: High
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2006-6627

cvss: 10.0
severity: Critical
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:L/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2007-0038

cvss: 9.3
severity: Critical
cwe: CWE-119
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2010-1425

cvss: 5.0
severity: Medium
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:L/Au:N/C:N/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'NONE', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2015-4950

cvss: 4.0
severity: Medium
cwe: CWE-200
cvss-vector: AV:N/AC:L/Au:S/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'SINGLE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2015-6557

cvss: 2.1
severity: Low
cwe: CWE-200
cvss-vector: AV:L/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'LOCAL'}

CVE-2015-7404

cvss: 1.9
severity: Low
cwe: CWE-200
cvss-vector: AV:L/AC:M/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'LOCAL'}
Rating: 10.0

193.136.173.5 - mx1.ua.pt

name: mx1.ua.pt
ports: {'open': {'25': {'type': 'tcp', 'state': 'open', 'service': 'smtp', 'version': 'MicrosoftExchangesmtpd'}, '1720': {'type': 'tcp', 'state': 'open', 'service': 'h323q931?', 'version': ''}}, 'Filtered': ' 998 filtered tcp ports '}
OS:
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', 'mx1.ua.pt': '193.136.173.5'}

CVE-2000-0122

cvss: 5.0
severity: Medium
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2000-0256

cvss: 7.5
severity: High
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2004-2383

cvss: 5.1
severity: Medium
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:H/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'HIGH', 'vector': 'NETWORK'}

CVE-2006-3942

cvss: 7.8
severity: High
cwe: CWE-20
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2006-5395

cvss: 7.5
severity: High
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2006-6627

cvss: 10.0
severity: Critical
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:L/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2007-0038

cvss: 9.3
severity: Critical
cwe: CWE-119
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2010-1425

cvss: 5.0
severity: Medium
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:L/Au:N/C:N/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'NONE', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2015-4950

cvss: 4.0
severity: Medium
cwe: CWE-200
cvss-vector: AV:N/AC:L/Au:S/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'SINGLE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2015-6557

cvss: 2.1
severity: Low
cwe: CWE-200
cvss-vector: AV:L/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'LOCAL'}

CVE-2015-7404

cvss: 1.9
severity: Low
cwe: CWE-200
cvss-vector: AV:L/AC:M/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'LOCAL'}
Rating: 10.0

193.136.173.6 - mx2.ua.pt

name: mx2.ua.pt
ports: {'open': {'25': {'type': 'tcp', 'state': 'open', 'service': 'smtp', 'version': 'MicrosoftExchangesmtpd'}, '1720': {'type': 'tcp', 'state': 'open', 'service': 'h323q931?', 'version': ''}}, 'Filtered': ' 998 filtered tcp ports '}
OS:
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', 'mx2.ua.pt': '193.136.173.6'}

CVE-2000-0122

cvss: 5.0
severity: Medium
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2000-0256

cvss: 7.5
severity: High
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2004-2383

cvss: 5.1
severity: Medium
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:H/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'HIGH', 'vector': 'NETWORK'}

CVE-2006-3942

cvss: 7.8
severity: High
cwe: CWE-20
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2006-5395

cvss: 7.5
severity: High
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2006-6627

cvss: 10.0
severity: Critical
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:L/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2007-0038

cvss: 9.3
severity: Critical
cwe: CWE-119
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2010-1425

cvss: 5.0
severity: Medium
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:L/Au:N/C:N/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'NONE', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2015-4950

cvss: 4.0
severity: Medium
cwe: CWE-200
cvss-vector: AV:N/AC:L/Au:S/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'SINGLE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2015-6557

cvss: 2.1
severity: Low
cwe: CWE-200
cvss-vector: AV:L/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'LOCAL'}

CVE-2015-7404

cvss: 1.9
severity: Low
cwe: CWE-200
cvss-vector: AV:L/AC:M/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'LOCAL'}
Rating: 10.0

192.168.253.125 - mx3.demo.ua.pt

name: mx3.demo.ua.pt
ports: {'open': {}, 'Filtered': ' 1000 filtered tcp ports '}
OS:
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', '10.1.0.92': '10.1.0.92', 'mx3.demo.ua.pt': '192.168.253.125'}
Rating: 0

193.136.173.26 - mx3.ua.pt

name: mx3.ua.pt
ports: {'open': {'25': {'type': 'tcp', 'state': 'open', 'service': 'smtp', 'version': 'IronPortsmtpd'}, '1720': {'type': 'tcp', 'state': 'open', 'service': 'h323q931?', 'version': ''}}, 'Filtered': ' 998 filtered tcp ports '}
OS: FreeBSD 9.0-RELEASE - 10.3-RELEASE
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', '10.1.0.92': '10.1.0.92', 'fw-vsdc.ua.pt': '193.137.173.236', 'mx3.ua.pt': '193.136.173.26'}

CVE-2009-0053

cvss: 4.3
severity: Medium
cwe: CWE-310
cvss-vector: AV:N/AC:M/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2009-0054

cvss: 4.3
severity: Medium
cwe: CWE-255
cvss-vector: AV:N/AC:M/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2009-0055

cvss: 6.8
severity: Medium

cwe: CWE-352
cvss-vector: AV:N/AC:M/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2009-0056

cvss: 6.8
severity: Medium
cwe: CWE-352
cvss-vector: AV:N/AC:M/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}
Rating: 6.8

193.136.173.27 - mx4.ua.pt

name: mx4.ua.pt
ports: {'open': {'25': {'type': 'tcp', 'state': 'open', 'service': 'smtp', 'version': 'IronPortsmtpd'}, '1720': {'type': 'tcp', 'state': 'open', 'service': 'h323q931?', 'version': ''}}, 'Filtered': ' 998 filtered tcp ports '}
OS: FreeBSD 9.0-RELEASE - 10.3-RELEASE
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', 'mx4.ua.pt': '193.136.173.27'}

CVE-2009-0053

cvss: 4.3
severity: Medium
cwe: CWE-310
cvss-vector: AV:N/AC:M/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2009-0054

cvss: 4.3
severity: Medium
cwe: CWE-255
cvss-vector: AV:N/AC:M/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2009-0055

cvss: 6.8
severity: Medium
cwe: CWE-352
cvss-vector: AV:N/AC:M/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2009-0056

cvss: 6.8
severity: Medium
cwe: CWE-352
cvss-vector: AV:N/AC:M/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}
Rating: 6.8

193.136.173.91 - naleph.doc.ua.pt

name: naleph.doc.ua.pt
ports: {'open': {'80': {'type': 'tcp', 'state': 'open', 'service': 'http', 'version': 'Apachehttpd2.4.7((Ubuntu))'}, '443': {'type': 'tcp', 'state': 'open', 'service': 'ssl/http',

'version': 'Apachehttpd2.4.7((Ubuntu))'}, '1720': {'type': 'tcp', 'state': 'open', 'service': 'h323q931?', 'version': ''}}, 'Filtered': ' 997 filtered tcp ports '}
OS:
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', '10.1.0.92': '10.1.0.92', 'fw-vsdc.ua.pt': '193.137.173.236', 'opac.ua.pt': '193.136.173.91'}

CVE-2019-13115

cvss: 5.8
severity: Medium
cwe: CWE-190
cvss-vector: AV:N/AC:M/Au:N/C:P/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}
Rating: 5.8

193.136.172.219 - next-online.ua.pt

name: next-online.ua.pt
ports: {'open': {'1720': {'type': 'tcp', 'state': 'open', 'service': 'h323q931?', 'version': ''}}, 'Filtered': ' 999 filtered tcp ports '}
OS: OpenBSD 4.0
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', 'sTIC-DigiQ.ua.pt': '193.136.172.219'}
Rating: 0

193.136.173.1 - oldmail.ua.pt

name: oldmail.ua.pt
ports: {'open': {'1720': {'type': 'tcp', 'state': 'open', 'service': 'h323q931?', 'version': ''}}, 'Filtered': ' 999 filtered tcp ports '}
OS: OpenBSD 4.0
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', 'cgpmail.ua.pt': '193.136.173.1'}
Rating: 0

192.168.248.176 - openstack.servers.ua.pt

name: openstack.servers.ua.pt
ports: {'open': {}, 'Filtered': ' 1000 filtered tcp ports '}
OS:
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', '10.1.0.92': '10.1.0.92', 'openstack.servers.ua.pt': '192.168.248.176'}
Rating: 0

192.168.160.202 - paco20-play.ua.pt

name: paco20-play.ua.pt
ports: {'open': {}, 'Filtered': ' 1000 filtered tcp ports '}
OS:
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', '10.1.0.92': '10.1.0.92', '10.1.0.42': '10.1.0.42', 'paco20-play.ua.pt': '192.168.160.202'}
Rating: 0

192.168.160.240 - paco20-prod.ua.pt

name: paco20-prod.ua.pt
ports: {'open': {}, 'Filtered': ' 1000 filtered tcp ports '}
OS:
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', '10.1.0.92': '10.1.0.92', '10.1.0.41': '10.1.0.41', 'paco20-prod.ua.pt': '192.168.160.240'}
Rating: 0

193.136.173.109 - pi4ies-g.ua.pt

name: pi4ies-g.ua.pt
ports: {'open': {'1720': {'type': 'tcp', 'state': 'open', 'service': 'h323q931?', 'version': ''}}, 'Filtered': ' 999 filtered tcp ports '}
OS: OpenBSD 4.0
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', 'pi4ies-puses.ua.pt': 'pi4ies-puses.ua.pt'}
Rating: 0

10.2.0.64 - prime.core.ua.pt

name: prime.core.ua.pt
ports: {'open': {}, 'Filtered': ' 1000 filtered tcp ports '}
OS:

Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', '10.1.0.92': '10.1.0.92', '10.1.0.10': '10.1.0.10', 'prime.core.ua.pt': '10.2.0.64'}
Rating: 0

193.136.172.76 - printing.ua.pt

name: printing.ua.pt
ports: {'open': {'1720': {'type': 'tcp', 'state': 'open', 'service': 'h323q931?', 'version': ''}}, 'Filtered': ' 999 filtered tcp ports '}
OS: OpenBSD 4.0
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', 'printing.ua.pt': '193.136.172.76'}
Rating: 0

193.136.172.42 - prismcentral.ua.pt

name: prismcentral.ua.pt
ports: {'open': {'80': {'type': 'tcp', 'state': 'open', 'service': 'http', 'version': 'envoy'}, '1720': {'type': 'tcp', 'state': 'open', 'service': 'h323q931?', 'version': ''}}, 'Filtered': ' 998 filtered tcp ports '}
OS: Linux 3.16
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', 'prismcentral.ua.pt': '193.136.172.42'}
Rating: 0

192.168.240.15 - quexs-isca.ua.pt

name: quexs-isca.ua.pt
ports: {'open': {}, 'Filtered': ' 1000 filtered tcp ports '}
OS:
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', '10.1.0.92': '10.1.0.92', 'campanhas.voip.ua.pt': '192.168.240.15'}
Rating: 0

192.92.133.54 - registry.dev.ua.pt

name: registry.dev.ua.pt
ports: {'open': {'1720': {'type': 'tcp', 'state': 'open', 'service': 'h323q931?', 'version': ''}}, 'Filtered': ' 999 filtered tcp ports '}
OS: OpenBSD 4.3
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', 'registry.dev.ua.pt': '192.92.133.54'}
Rating: 0

193.136.172.207 - reyka.ua.pt

name: reyka.ua.pt
ports: {'open': {'1720': {'type': 'tcp', 'state': 'open', 'service': 'h323q931?', 'version': ''}, '2179': {'type': 'tcp', 'state': 'open', 'service': 'vmrdp?', 'version': ''}}, 'Filtered': ' 998 filtered tcp ports '}
OS: OpenBSD 4.0
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', 'reyka.ua.pt': '193.136.172.207'}
Rating: 0

193.137.172.66 - sas-desporto.ua.pt

name: sas-desporto.ua.pt
ports: {'open': {'22': {'type': 'tcp', 'state': 'open', 'service': 'ssh', 'version': 'OpenSSH7.6p1Ubuntu4ubuntu0.3(UbuntuLinux;protocol2.0)'}, '80': {'type': 'tcp', 'state': 'open', 'service': 'http', 'version': 'Apachehttpd2.4.29'}, '443': {'type': 'tcp', 'state': 'open', 'service': 'ssl/http', 'version': 'Apachehttpd2.4.29((Ubuntu))'}, '8080': {'type': 'tcp', 'state': 'closed', 'service': 'http-proxy', 'version': ''}}, 'Filtered': ' 996 filtered tcp ports '}
OS: Linux 2.6.32
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', '10.1.0.92': '10.1.0.92', 'sas-desporto.ua.pt': '193.137.172.66'}

CVE-2016-10012

cvss: 7.2
severity: High
cwe: CWE-119
cvss-vector: AV:L/AC:L/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'LOCAL'}

CVE-2019-13115

cvss: 5.8
severity: Medium
cwe: CWE-190
cvss-vector: AV:N/AC:M/Au:N/C:P/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}
Rating: 7.2

193.136.172.156 - scom-w2.ua.pt

name: scom-w2.ua.pt
ports: {'open': {'1720': {'type': 'tcp', 'state': 'open', 'service': 'h323q931?', 'version': ''}}, 'Filtered': ' 999 filtered tcp ports '}
OS: OpenBSD 4.0
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', 'scom-w2.ua.pt': '193.136.172.156'}
Rating: 0

193.136.173.24 - seonline.isca.ua.pt

name: seonline.isca.ua.pt
ports: {'open': {'80': {'type': 'tcp', 'state': 'open', 'service': 'http', 'version': 'MicrosoftHTTPAPIhttpd2.0(SSDP/UPnP)'}, '443': {'type': 'tcp', 'state': 'open', 'service': 'ssl/http', 'version': 'MicrosoftHTTPAPIhttpd2.0(SSDP/UPnP)'}, '1720': {'type': 'tcp', 'state': 'open', 'service': 'h323q931?', 'version': ''}}, 'Filtered': ' 997 filtered tcp ports '}
OS: AVtech Room Alert 26W environmental monitor
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', '10.1.0.92': '10.1.0.92', 'fw-vsdc.ua.pt': '193.137.173.236', 'srv-isca-aulas.ua.pt': '193.136.173.24'}

CVE-2000-0122

cvss: 5.0
severity: Medium
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2006-6627

cvss: 10.0
severity: Critical
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:L/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2008-1447

cvss: 5.0
severity: Medium
cwe: CWE-331
cvss-vector: AV:N/AC:L/Au:N/C:N/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'NONE', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2009-0087

cvss: 9.3
severity: Critical
cwe: NVD-CWE-noinfo
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2009-0100

cvss: 9.3
severity: Critical
cwe: CWE-399
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2009-0550

cvss: 9.3
severity: Critical
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2009-0557

cvss: 9.3
severity: Critical
cwe: CWE-94
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2009-0560

cvss: 9.3
severity: Critical
cwe: CWE-399
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2009-0561

cvss: 9.3
severity: Critical
cwe: CWE-189
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2009-0563

cvss: 9.3
severity: Critical
cwe: CWE-119
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2009-0565

cvss: 9.3
severity: Critical
cwe: CWE-119
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2009-2499

cvss: 8.5
severity: High
cwe: CWE-94
cvss-vector: AV:N/AC:M/Au:S/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'SINGLE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2010-1900

cvss: 9.3
severity: Critical
cwe: CWE-94
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2010-1901

cvss: 9.3
severity: Critical
cwe: CWE-94
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2010-1902

cvss: 9.3
severity: Critical
cwe: CWE-119
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2015-4950

cvss: 4.0
severity: Medium
cwe: CWE-200
cvss-vector: AV:N/AC:L/Au:S/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'SINGLE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2017-0098

cvss: 2.9
severity: Low
cwe: CWE-20
cvss-vector: AV:A/AC:M/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'ADJACENT_NETWORK'}

CVE-2018-5391

cvss: 7.8
severity: High
cwe: CWE-20
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2020-26233

cvss: 3.6
severity: Low
cwe: CWE-706
cvss-vector: AV:N/AC:H/Au:S/C:P/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'SINGLE', 'complexity': 'HIGH', 'vector': 'NETWORK'}

CVE-2020-35608

cvss: 7.2
severity: High
cwe: CWE-74
cvss-vector: AV:L/AC:L/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'LOCAL'}

CVE-2021-21505

cvss: 10.0
severity: Critical
cwe: CWE-522
cvss-vector: AV:N/AC:L/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-44228

cvss: 9.3
severity: Critical
cwe: CWE-502
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}
Rating: 10.0

193.137.172.72 - sga-mobilidadenet-qa.ua.pt

name: sga-mobilidadenet-qa.ua.pt
ports: {'open': {'80': {'type': 'tcp', 'state': 'open', 'service': 'http', 'version': 'nginx1.20.1'}, '443': {'type': 'tcp', 'state': 'open', 'service': 'ssl/http', 'version': 'nginx1.20.1'}}, 'Filtered': ' 998 filtered tcp ports '}
OS:
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', '10.1.0.92': '10.1.0.92', 'sga-mobilidadenet-qa.ua.pt': '193.137.172.72'}
Rating: 0

193.137.172.68 - sga-mobilidadenet.ua.pt

name: sga-mobilidadenet.ua.pt
ports: {'open': {'80': {'type': 'tcp', 'state': 'open', 'service': 'http', 'version': 'nginx1.20.1'}, '443': {'type': 'tcp', 'state': 'open', 'service': 'ssl/http', 'version': 'nginx1.20.1'}}, 'Filtered': ' 998 filtered tcp ports '}
OS:
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', '10.1.0.92': '10.1.0.92', 'sga-mobilidadenet.ua.pt': '193.137.172.68'}
Rating: 0

193.136.173.92 - sigb.ua.pt

name: sigb.ua.pt
ports: {'open': {'1720': {'type': 'tcp', 'state': 'open', 'service': 'h323q931?', 'version': ''}}, 'Filtered': ' 999 filtered tcp ports '}
OS: OpenBSD 4.0
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', 'sigb.ua.pt': '193.136.173.92'}
Rating: 0

193.136.173.78 - sma.ua.pt

name: sma.ua.pt
ports: {'open': {'1720': {'type': 'tcp', 'state': 'open', 'service': 'h323q931?', 'version': ''}}, 'Filtered': ' 999 filtered tcp ports '}
OS: OpenBSD 4.0

Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', 'sma.ua.pt': '193.136.173.78'}
Rating: 0

193.136.172.120 - snapcreator.ua.pt

name: snapcreator.ua.pt
ports: {'open': {'1720': {'type': 'tcp', 'state': 'open', 'service': 'h323q931?', 'version': ''}}, 'Filtered': ' 999 filtered tcp ports '}
OS: OpenBSD 4.0
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', 'snapcreator.ua.pt': '193.136.172.120'}
Rating: 0

193.136.172.151 - srv-sccm2012.ua.pt

name: srv-sccm2012.ua.pt
ports: {'open': {'80': {'type': 'tcp', 'state': 'open', 'service': 'http', 'version': 'MicrosoftIIShttpd8.5'}, '443': {'type': 'tcp', 'state': 'open', 'service': 'https?', 'version': ''}, '1720': {'type': 'tcp', 'state': 'open', 'service': 'h323q931?', 'version': ''}}, 'Filtered': ' 997 filtered tcp ports '}
OS:
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', '10.1.0.92': '10.1.0.92', 'fw-vsdc.ua.pt': '193.137.173.236', 'srv-sccm2012.ua.pt': '193.136.172.151'}

CVE-1999-0488

cvss: 7.5
severity: High
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2000-0122

cvss: 5.0
severity: Medium
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2000-0160

cvss: 7.6
severity: High
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:H/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'HIGH', 'vector': 'NETWORK'}

CVE-2000-0256

cvss: 7.5
severity: High
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2000-0544

cvss: 5.0
severity: Medium
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2002-0419

cvss: 5.0
severity: Medium
cwe: CWE-200
cvss-vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2004-0790

cvss: 5.0
severity: Medium
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2004-0928

cvss: 5.0
severity: Medium
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2004-1060

cvss: 5.0
severity: Medium
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2004-2383

cvss: 5.1
severity: Medium
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:H/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'HIGH', 'vector': 'NETWORK'}

CVE-2005-0563

cvss: 4.3
severity: Medium
cwe: CWE-79
cvss-vector: AV:N/AC:M/Au:N/C:N/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'NONE', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2006-3697

cvss: 7.2
severity: High
cwe: CWE-264
cvss-vector: AV:L/AC:L/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'LOCAL'}

CVE-2006-3942

cvss: 7.8
severity: High
cwe: CWE-20
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2006-5395

cvss: 7.5
severity: High
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2006-6627

cvss: 10.0
severity: Critical
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:L/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2007-0038

cvss: 9.3
severity: Critical
cwe: CWE-119
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2007-1765

cvss: 9.3
severity: Critical
cwe: NVD-CWE-noinfo
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2007-6502

cvss: 5.5
severity: Medium
cwe: CWE-200
cvss-vector: AV:N/AC:L/Au:S/C:P/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'SINGLE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2008-0085

cvss: 5.0
severity: Medium
cwe: CWE-200
cvss-vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2008-0107

cvss: 9.0
severity: Critical
cwe: CWE-189
cvss-vector: AV:N/AC:L/Au:S/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'SINGLE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2008-1447

cvss: 5.0
severity: Medium
cwe: CWE-331
cvss-vector: AV:N/AC:L/Au:N/C:N/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'NONE', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2008-3243

cvss: 4.3
severity: Medium
cwe: CWE-20
cvss-vector: AV:N/AC:M/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2009-0087

cvss: 9.3
severity: Critical
cwe: NVD-CWE-noinfo
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2009-0100

cvss: 9.3
severity: Critical
cwe: CWE-399
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2009-0550

cvss: 9.3
severity: Critical
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2009-0557

cvss: 9.3
severity: Critical
cwe: CWE-94
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2009-0560

cvss: 9.3
severity: Critical
cwe: CWE-399
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2009-0561

cvss: 9.3
severity: Critical
cwe: CWE-189
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2009-0563

cvss: 9.3
severity: Critical
cwe: CWE-119
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2009-0565

cvss: 9.3
severity: Critical
cwe: CWE-119
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2009-1134

cvss: 9.3
severity: Critical
cwe: CWE-94
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2009-2499

cvss: 8.5
severity: High
cwe: CWE-94
cvss-vector: AV:N/AC:M/Au:S/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'SINGLE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2010-1263

cvss: 9.3
severity: Critical
cwe: CWE-94
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2010-1425

cvss: 5.0
severity: Medium
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:L/Au:N/C:N/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'NONE', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2010-1900

cvss: 9.3
severity: Critical
cwe: CWE-94
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2010-1901

cvss: 9.3
severity: Critical
cwe: CWE-94
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2010-1902

cvss: 9.3
severity: Critical
cwe: CWE-119
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2012-1854

cvss: 6.9
severity: Medium
cwe: NVD-CWE-Other
cvss-vector: AV:L/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'LOCAL'}

CVE-2015-4950

cvss: 4.0
severity: Medium
cwe: CWE-200
cvss-vector: AV:N/AC:L/Au:S/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'SINGLE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2015-6557

cvss: 2.1
severity: Low
cwe: CWE-200
cvss-vector: AV:L/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'LOCAL'}

CVE-2015-7404

cvss: 1.9
severity: Low
cwe: CWE-200
cvss-vector: AV:L/AC:M/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'LOCAL'}

CVE-2017-0098

cvss: 2.9
severity: Low
cwe: CWE-20
cvss-vector: AV:A/AC:M/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'ADJACENT_NETWORK'}

CVE-2018-5282

cvss: 7.2
severity: High
cwe: CWE-787
cvss-vector: AV:L/AC:L/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'LOCAL'}

CVE-2018-5391

cvss: 7.8
severity: High
cwe: CWE-20
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-1000

cvss: 3.5
severity: Low
cwe: CWE-269
cvss-vector: AV:N/AC:M/Au:S/C:N/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'NONE', 'integrity': 'PARTIAL'}
access: {'authentication': 'SINGLE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2019-16863

cvss: 4.3
severity: Medium
cwe: CWE-327
cvss-vector: AV:N/AC:M/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2020-1296

cvss: 2.1
severity: Low
cwe: CWE-200
cvss-vector: AV:L/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'LOCAL'}

CVE-2020-1459

cvss: 2.1
severity: Low
cwe: CWE-200
cvss-vector: AV:L/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'LOCAL'}

CVE-2020-26233

cvss: 3.6
severity: Low
cwe: CWE-706
cvss-vector: AV:N/AC:H/Au:S/C:P/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'SINGLE', 'complexity': 'HIGH', 'vector': 'NETWORK'}

CVE-2020-35608

cvss: 7.2
severity: High
cwe: CWE-74
cvss-vector: AV:L/AC:L/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'LOCAL'}

CVE-2021-21505

cvss: 10.0
severity: Critical
cwe: CWE-522
cvss-vector: AV:N/AC:L/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-38505

cvss: 4.3
severity: Medium
cwe: CWE-668
cvss-vector: AV:N/AC:M/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2021-44228

cvss: 9.3
severity: Critical
cwe: CWE-502
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}
Rating: 10.0

192.168.160.241 - ssc.web.ua.pt

name: ssc.web.ua.pt
ports: {'open': {}, 'Filtered': ' 1000 filtered tcp ports '}
OS:
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', '10.1.0.92': '10.1.0.92', '10.1.0.41': '10.1.0.41', 'pi2020-g5.ua.pt': '192.168.160.241'}
Rating: 0

192.168.160.193 - staging-nextcloud1.ua.pt

name: staging-nextcloud1.ua.pt
ports: {'open': {}, 'Filtered': ' 1000 filtered tcp ports '}
OS:
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', '10.1.0.92': '10.1.0.92', '10.1.0.41': '10.1.0.41', 'staging-nextcloud1.ua.pt': '192.168.160.193'}
Rating: 0

193.136.173.65 - stic-openid.ua.pt

name: stic-openid.ua.pt
ports: {'open': {'1720': {'type': 'tcp', 'state': 'open', 'service': 'h323q931?', 'version': ''}}, 'Filtered': ' 999 filtered tcp ports '}
OS: OpenBSD 4.0
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', 'stic-openid.ua.pt': '193.136.173.65'}
Rating: 0

10.55.15.15 - stic-pam-pta.ua.pt

name: stic-pam-pta.ua.pt
ports: {'open': {'1720': {'type': 'tcp', 'state': 'open', 'service': 'h323q931?', 'version': ''}}, 'Filtered': ' 999 filtered tcp ports '}
OS: OpenBSD 4.0
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', 'stic-pam-pta.ua.pt': '10.55.15.15'}
Rating: 0

10.55.15.16 - stic-pam.ua.pt

name: stic-pam.ua.pt
ports: {'open': {'1720': {'type': 'tcp', 'state': 'open', 'service': 'h323q931?', 'version': ''}}, 'Filtered': ' 999 filtered tcp ports '}
OS: OpenBSD 4.0
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', 'stic-pam.ua.pt': '10.55.15.16'}
Rating: 0

193.136.172.49 - stic-vmportal.ua.pt

name: stic-vmportal.ua.pt
ports: {'open': {'443': {'type': 'tcp', 'state': 'open', 'service': 'ssl/http', 'version': 'MicrosoftIIShttpd10.0'}, '1720': {'type': 'tcp', 'state': 'open', 'service': 'h323q931?', 'version': ''}}, 'Filtered': ' 998 filtered tcp ports '}
OS: AVtech Room Alert 26W environmental monitor
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', 'stic-vmportal.ua.pt': '193.136.172.49'}

CVE-2021-38505

cvss: 4.3
severity: Medium
cwe: CWE-668
cvss-vector: AV:N/AC:M/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}
Rating: 4.3

192.168.181.1 - stolichnaya-vip.ua.pt

name: stolichnaya-vip.ua.pt
ports: {'open': {}, 'Filtered': ' 1000 filtered tcp ports '}
OS:
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', '10.1.0.92': '10.1.0.92', 'fw-vsdc.ua.pt': '193.137.173.236', 'stolichnaya-vip.ua.pt': '192.168.181.1'}
Rating: 0

193.136.172.183 - tfs.clients.ua.pt

name: tfs.clients.ua.pt
ports: {'open': {'80': {'type': 'tcp', 'state': 'open', 'service': 'http', 'version': 'MicrosoftHTTPAPIhttpd2.0(SSDP/UPnP)'}, '443': {'type': 'tcp', 'state': 'open', 'service': 'ssl/http', 'version': 'MicrosoftHTTPAPIhttpd2.0(SSDP/UPnP)'}, '1720': {'type': 'tcp', 'state': 'open', 'service': 'h323q931?', 'version': ''}}, 'Filtered': ' 997 filtered tcp ports '}
OS:
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', 'tfs.clients.ua.pt': '193.136.172.183'}

CVE-2000-0122

cvss: 5.0
severity: Medium
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2006-6627

cvss: 10.0
severity: Critical
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:L/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2008-1447

cvss: 5.0
severity: Medium
cwe: CWE-331
cvss-vector: AV:N/AC:L/Au:N/C:N/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'NONE', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2009-0087

cvss: 9.3
severity: Critical
cwe: NVD-CWE-noinfo
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2009-0100

cvss: 9.3
severity: Critical
cwe: CWE-399
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2009-0550

cvss: 9.3
severity: Critical
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2009-0557

cvss: 9.3
severity: Critical
cwe: CWE-94
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2009-0560

cvss: 9.3
severity: Critical
cwe: CWE-399
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2009-0561

cvss: 9.3
severity: Critical
cwe: CWE-189
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2009-0563

cvss: 9.3
severity: Critical
cwe: CWE-119
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2009-0565

cvss: 9.3
severity: Critical
cwe: CWE-119
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2009-2499

cvss: 8.5
severity: High
cwe: CWE-94
cvss-vector: AV:N/AC:M/Au:S/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'SINGLE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2010-1900

cvss: 9.3
severity: Critical
cwe: CWE-94
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2010-1901

cvss: 9.3
severity: Critical
cwe: CWE-94
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2010-1902

cvss: 9.3
severity: Critical
cwe: CWE-119
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2015-4950

cvss: 4.0
severity: Medium
cwe: CWE-200
cvss-vector: AV:N/AC:L/Au:S/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'SINGLE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2017-0098

cvss: 2.9
severity: Low
cwe: CWE-20
cvss-vector: AV:A/AC:M/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'ADJACENT_NETWORK'}

CVE-2018-5391

cvss: 7.8
severity: High
cwe: CWE-20
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2020-26233

cvss: 3.6
severity: Low
cwe: CWE-706
cvss-vector: AV:N/AC:H/Au:S/C:P/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'SINGLE', 'complexity': 'HIGH', 'vector': 'NETWORK'}

CVE-2020-35608

cvss: 7.2
severity: High
cwe: CWE-74
cvss-vector: AV:L/AC:L/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'LOCAL'}

CVE-2021-21505

cvss: 10.0
severity: Critical
cwe: CWE-522
cvss-vector: AV:N/AC:L/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-44228

cvss: 9.3
severity: Critical
cwe: CWE-502
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}
Rating: 10.0

10.2.1.26 - ucs6248up.core.ua.pt

name: ucs6248up.core.ua.pt
ports: {'open': {}, 'Filtered': ' 1000 filtered tcp ports '}
OS:
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', '10.1.0.92': '10.1.0.92', '10.1.0.9': '10.1.0.9', 'ucs6248up.core.ua.pt': '10.2.1.26'}
Rating: 0

192.168.181.73 - virtualapps-i.ua.pt

name: virtualapps-i.ua.pt
ports: {'open': {}, 'Filtered': ' 1000 filtered tcp ports '}
OS:
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', '10.1.0.92': '10.1.0.92', 'fw-vsdc.ua.pt': '193.137.173.236', 'virtualapps-i.ua.pt': '192.168.181.73'}
Rating: 0

193.136.173.118 - virtualapps.ua.pt

name: virtualapps.ua.pt
ports: {'open': {'1720': {'type': 'tcp', 'state': 'open', 'service': 'h323q931?', 'version': ''}}, 'Filtered': ' 999 filtered tcp ports '}
OS: OpenBSD 4.0
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', '193.136.173.118': '193.136.173.118'}
Rating: 0

192.168.240.27 - voip.ua.pt

name: voip.ua.pt
ports: {'open': {}, 'Filtered': ' 1000 filtered tcp ports '}
OS:
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', '10.1.0.92': '10.1.0.92', 'ipbxuaveiro.voip.ua.pt': '192.168.240.27'}
Rating: 0

192.92.133.28 - wavecom.voip.ua.pt

name: wavecom.voip.ua.pt
ports: {'open': {'1720': {'type': 'tcp', 'state': 'open', 'service': 'h323q931?', 'version': ''}}, 'Filtered': ' 999 filtered tcp ports '}
OS: OpenBSD 4.0
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', '192.92.133.28': '192.92.133.28'}
Rating: 0

192.92.133.36 - wso2-1.dev.ua.pt

name: wso2-1.dev.ua.pt
ports: {'open': {'1720': {'type': 'tcp', 'state': 'open', 'service': 'h323q931?', 'version': ''}}, 'Filtered': ' 999 filtered tcp ports '}
OS: OpenBSD 4.0
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', 'wso2-1.dev.ua.pt': '192.92.133.36'}
Rating: 0

193.136.92.35 - 4tellstore.av.it.pt

name: 4tellstore.av.it.pt
ports: {'open': {'22': {'type': 'tcp', 'state': 'open', 'service': 'ssh', 'version': 'OpenSSH6.1(protocol2.0)'}, '80': {'type': 'tcp', 'state': 'open', 'service': 'http', 'version': 'Apachehttpd(PHP5.3.28)'}, '443': {'type': 'tcp', 'state': 'open', 'service': 'ssl/http', 'version': 'QNAPNAShttpconfig'}, '631': {'type': 'tcp', 'state': 'open', 'service': 'ipp', 'version': 'CUPS1.6'}, '873': {'type': 'tcp', 'state': 'open', 'service': 'rsync', 'version': '(protocolversion30)'}, '8080': {'type': 'tcp', 'state': 'open', 'service': 'http', 'version': 'Apachehttpd'}, '8081': {'type': 'tcp', 'state': 'open', 'service': 'ssl/http', 'version': 'Apachehttpd(PHP5.3.28)'}, '8200': {'type': 'tcp', 'state': 'open', 'service': 'upnp',

'version': 'QNAPDLNA1.0(DLNADOC1.50;UPnP1.0)'}, '49152': {'type': 'tcp', 'state': 'open', 'service': 'upnp', 'version': 'PortableSDKforUPnPdevices1.6.18(Linux3.4.6;UPnP1.0)'}}, 'Filtered': ' 991 closed tcp ports '}
OS:
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', '4tellstore.av.it.pt': '193.136.92.35'}

CVE-2012-0814

cvss: 3.5
severity: Low
cwe: CWE-255
cvss-vector: AV:N/AC:M/Au:S/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'SINGLE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2016-10012

cvss: 7.2
severity: High
cwe: CWE-119
cvss-vector: AV:L/AC:L/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'LOCAL'}

CVE-2016-10708

cvss: 5.0
severity: Medium
cwe: CWE-476
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}
Rating: 7.2

193.136.92.150 - alex.aws.atnog.av.it.pt

name: alex.aws.atnog.av.it.pt
ports: {'open': {'22': {'type': 'tcp', 'state': 'open', 'service': 'ssh', 'version': 'OpenSSH8.2p1Ubuntu4ubuntu0.4(UbuntuLinux;protocol2.0)'}, '80': {'type': 'tcp', 'state': 'open', 'service': 'http', 'version': 'nginx'}, '111': {'type': 'tcp', 'state': 'open', 'service': 'rpcbind', 'version': '2-4(RPC#100000)'}, '443': {'type': 'tcp', 'state': 'open', 'service': 'ssl/http', 'version': 'nginx'}, '8080': {'type': 'tcp', 'state': 'open', 'service': 'http', 'version': 'nginx'}, '8081': {'type': 'tcp', 'state': 'open', 'service': 'ssl/http', 'version': 'nginx'}, '8082': {'type': 'tcp', 'state': 'open', 'service': 'http', 'version': 'nginx'}}, 'Filtered': ' 993 closed tcp ports '}
OS:
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', 'athena.av.it.pt': '193.136.92.150'}

CVE-2012-0814

cvss: 3.5
severity: Low
cwe: CWE-255
cvss-vector: AV:N/AC:M/Au:S/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'SINGLE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2016-10012

cvss: 7.2
severity: High
cwe: CWE-119
cvss-vector: AV:L/AC:L/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'LOCAL'}

CVE-2016-10708

cvss: 5.0
severity: Medium
cwe: CWE-476
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}
Rating: 7.2

10.0.10.90 - claudia.av.it.pt

name: claudia.av.it.pt
ports: {'open': {'22': {'type': 'tcp', 'state': 'open', 'service': 'ssh', 'version': 'OpenSSH8.0(protocol2.0)'}, '25': {'type': 'tcp', 'state': 'open', 'service': 'tcpwrapped', 'version': ''}, '80': {'type': 'tcp', 'state': 'open', 'service': 'http', 'version': 'MicrosoftIIShttpd10.0'}, '111': {'type': 'tcp', 'state': 'open', 'service': 'rpcbind', 'version': '2-4(RPC#100000)'}, '135': {'type': 'tcp', 'state': 'open', 'service': 'msrpc', 'version': 'MicrosoftWindowsRPC'}, '139': {'type': 'tcp', 'state': 'open', 'service': 'netbios-ssn', 'version': 'MicrosoftWindowsnetbios-ssn'}, '443': {'type': 'tcp', 'state': 'open', 'service': 'https?', 'version': ''}, '445': {'type': 'tcp', 'state': 'open', 'service': 'microsoft-ds', 'version': 'MicrosoftWindowsServer2008R2-2012microsoft-ds(workgroup:AV)'}, '587': {'type': 'tcp', 'state': 'open', 'service': 'tcpwrapped', 'version': ''}, '2049': {'type': 'tcp', 'state': 'open', 'service': 'mountd', 'version': '1-3(RPC#100005)'}, '3260': {'type': 'tcp', 'state': 'open', 'service': 'iscsi?', 'version': ''}, '3389': {'type': 'tcp', 'state': 'open', 'service': 'ms-wbt-server', 'version': 'MicrosoftTerminalServices'}}, 'Filtered': ' 988 filtered tcp ports '}
OS:
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', 'atnog-docstorage.av.it.pt': '10.0.10.90'}

CVE-2012-0814

cvss: 3.5
severity: Low
cwe: CWE-255
cvss-vector: AV:N/AC:M/Au:S/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'SINGLE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2016-10012

cvss: 7.2
severity: High
cwe: CWE-119
cvss-vector: AV:L/AC:L/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'LOCAL'}

CVE-2016-10708

cvss: 5.0
severity: Medium
cwe: CWE-476
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-38505

cvss: 4.3
severity: Medium
cwe: CWE-668
cvss-vector: AV:N/AC:M/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}
Rating: 7.2

10.0.20.15 - cloud.nap.av.it.pt

name: cloud.nap.av.it.pt
ports: {'open': {}, 'Filtered': ' 1000 filtered tcp ports '}
OS:
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', 'nap-gw01.av.it.pt': '193.136.93.20', 'code.nap.av.it.pt': '10.0.20.15'}
Rating: 0

193.136.92.140 - es.av.it.pt

name: es.av.it.pt
ports: {'open': {'21': {'type': 'tcp', 'state': 'closed', 'service': 'ftp', 'version': ''}, '22': {'type': 'tcp', 'state': 'open', 'service': 'ssh', 'version': 'OpenSSH8.9(protocol2.0)'}, '25': {'type': 'tcp', 'state': 'open', 'service': 'smtp', 'version': 'Eximsmtpd4.95'}, '53': {'type': 'tcp', 'state': 'closed', 'service': 'domain', 'version': ''}, '80': {'type': 'tcp', 'state': 'open', 'service': 'http', 'version': 'nginx'}, '443': {'type': 'tcp', 'state': 'open', 'service': 'ssl/http', 'version': 'nginx'}, '465': {'type': 'tcp', 'state': 'open', 'service': 'tcpwrapped', 'version': ''}, '587': {'type': 'tcp', 'state': 'open', 'service': 'smtp', 'version': 'Eximsmtpd4.95'}, '3306': {'type': 'tcp', 'state': 'open', 'service': 'mysql', 'version': 'MariaDB(unauthorized)'}, '5000': {'type': 'tcp', 'state': 'open', 'service': 'ssl/http', 'version': 'DockerRegistry(API:2.0)'}, '8080': {'type': 'tcp', 'state': 'closed', 'service': 'http-proxy', 'version': ''}, '9000': {'type': 'tcp', 'state': 'open', 'service': 'http', 'version': 'nginx1.19.7'}, '9001': {'type': 'tcp', 'state': 'open', 'service': 'http', 'version': 'nginx'}}, 'Filtered': ' 986 filtered tcp ports '}
OS: Linux 2.6.32
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', 'es.av.it.pt': '193.136.92.140'}

CVE-2012-0814

cvss: 3.5
severity: Low
cwe: CWE-255
cvss-vector: AV:N/AC:M/Au:S/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'SINGLE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2016-10012

cvss: 7.2
severity: High
cwe: CWE-119
cvss-vector: AV:L/AC:L/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'LOCAL'}

CVE-2016-10708

cvss: 5.0
severity: Medium
cwe: CWE-476
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2020-28025

cvss: 5.0
severity: Medium
cwe: CWE-125
cvss-vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}
Rating: 7.2

193.136.92.113 - fpga.av.it.pt

name: fpga.av.it.pt
ports: {'open': {'22': {'type': 'tcp', 'state': 'open', 'service': 'ssh', 'version': 'OpenSSH7.6p1Ubuntu4ubuntu0.6(UbuntuLinux;protocol2.0)'}, '25': {'type': 'tcp', 'state': 'open', 'service': 'smtp', 'version': 'Eximsmtpd4.90_1'}, '53': {'type': 'tcp', 'state': 'open', 'service': 'domain', 'version': 'ISCBIND9.11.3-1ubuntu1.17(UbuntuLinux)'}, '80': {'type': 'tcp', 'state': 'open', 'service': 'http', 'version': 'Apachehttpd'}, '111': {'type': 'tcp', 'state': 'open', 'service': 'rpcbind', 'version': '2-4(RPC#100000)'}, '443': {'type': 'tcp', 'state': 'open', 'service': 'ssl/http', 'version': 'Apachehttpd'}, '3306': {'type': 'tcp', 'state': 'open', 'service': 'mysql', 'version': 'MySQL(unauthorized)'}}, 'Filtered': ' 993 closed tcp ports '}
OS:
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', 'fpga.av.it.pt': '193.136.92.113'}

CVE-2016-10012

cvss: 7.2
severity: High
cwe: CWE-119
cvss-vector: AV:L/AC:L/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'LOCAL'}

CVE-2020-28025

cvss: 5.0
severity: Medium
cwe: CWE-125
cvss-vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2020-1992

cvss: 9.3
severity: Critical
cwe: CWE-134
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2020-2030

cvss: 9.0
severity: Critical
cwe: CWE-78
cvss-vector: AV:N/AC:L/Au:S/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'SINGLE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2020-26195

cvss: 5.0
severity: Medium
cwe: CWE-755
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-21502

cvss: 7.5
severity: High
cwe: CWE-269
cvss-vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}
Rating: 9.3

10.0.12.21 - iot.av.it.pt

name: iot.av.it.pt
ports: {'open': {'22': {'type': 'tcp', 'state': 'open', 'service': 'ssh', 'version': 'OpenSSH8.2p1Ubuntu4ubuntu0.3(UbuntuLinux;protocol2.0)'}, '80': {'type': 'tcp', 'state': 'open', 'service': 'http', 'version': 'nginx1.21.5'}, '111': {'type': 'tcp', 'state': 'open', 'service': 'rpcbind', 'version': '2-4(RPC#100000)'}, '3000': {'type': 'tcp', 'state': 'open', 'service': 'ssl/ppp?', 'version': ''}, '7777': {'type': 'tcp', 'state': 'open', 'service': 'http', 'version': 'Cowboyhttpd'}, '8080': {'type': 'tcp', 'state': 'open', 'service': 'rtsp', 'version': ''}, '8443': {'type': 'tcp', 'state': 'open', 'service': 'ssl/rtsp', 'version': ''}, '8888': {'type': 'tcp', 'state': 'open', 'service': 'amqp', 'version': 'RabbitMQ3.7.8(0-9)'}, '9090': {'type': 'tcp', 'state': 'open', 'service': 'http', 'version': 'Golangnet/httpserver(Go-IPFSjson-rpcorInfluxDBAPI)'}}, 'Filtered': ' 991 closed tcp ports '}
OS:
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', 'iot.av.it.pt': '10.0.12.21'}

CVE-2012-0814

cvss: 3.5
severity: Low
cwe: CWE-255
cvss-vector: AV:N/AC:M/Au:S/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'SINGLE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2016-10012

cvss: 7.2
severity: High
cwe: CWE-119
cvss-vector: AV:L/AC:L/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'LOCAL'}

CVE-2016-10708

cvss: 5.0
severity: Medium
cwe: CWE-476
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}
Rating: 7.2

193.136.92.181 - mephisto.av.it.pt

name: mephisto.av.it.pt
ports: {'open': {'22': {'type': 'tcp', 'state': 'open', 'service': 'ssh', 'version': 'OpenSSH7.9p1Debian10+deb10u2(protocol2.0)'}, '143': {'type': 'tcp', 'state': 'open', 'service': 'imap', 'version': 'Dovecotimapd'}, '993': {'type': 'tcp', 'state': 'open', 'service': 'ssl/imap', 'version': 'Dovecotimapd'}, '8080': {'type': 'tcp', 'state': 'open', 'service': 'http', 'version': 'ApacheTomcat'}}, 'Filtered': ' 996 closed tcp ports '}
OS:
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', 'mephisto.av.it.pt': '193.136.92.181'}

CVE-2016-10012

cvss: 7.2
severity: High
cwe: CWE-119
cvss-vector: AV:L/AC:L/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'LOCAL'}
Rating: 7.2

193.136.92.162 - onlyoffice.av.it.pt

name: onlyoffice.av.it.pt
ports: {'open': {'22': {'type': 'tcp', 'state': 'open', 'service': 'ssh', 'version': 'OpenSSH7.6p1Ubuntu4ubuntu0.5(UbuntuLinux;protocol2.0)'}, '25': {'type': 'tcp', 'state': 'open', 'service': 'smtp', 'version': 'Postfixsmtpd'}, '80': {'type': 'tcp', 'state': 'open', 'service': 'http', 'version': 'nginx'}, '143': {'type': 'tcp', 'state': 'open', 'service': 'imap', 'version': 'Dovecotimapd'}, '443': {'type': 'tcp', 'state': 'open', 'service': 'ssl/http', 'version': 'nginx'}, '587': {'type': 'tcp', 'state': 'open', 'service': 'smtp', 'version': 'Postfixsmtpd'}, '5222': {'type': 'tcp', 'state': 'open', 'service': 'xmpp-client?', 'version': ''}}, 'Filtered': ' 993 closed tcp ports '}
OS:
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', 'onlyoffice.av.it.pt': '193.136.92.162'}

CVE-2016-10012

cvss: 7.2
severity: High
cwe: CWE-119
cvss-vector: AV:L/AC:L/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'LOCAL'}

CVE-2021-33912

cvss: 9.3
severity: Critical
cwe: CWE-787
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2021-33913

cvss: 9.3
severity: Critical
cwe: CWE-787
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}
Rating: 9.3

193.136.92.1 - vpn2.av.it.pt

name: vpn2.av.it.pt
ports: {'open': {'22': {'type': 'tcp', 'state': 'open', 'service': 'ssh', 'version': 'OpenSSH7.5(protocol2.0)'}, '80': {'type': 'tcp', 'state': 'open', 'service': 'http', 'version': 'nginx'}, '443': {'type': 'tcp', 'state': 'open', 'service': 'ssl/http', 'version': 'nginx'}, '3000': {'type': 'tcp', 'state': 'open', 'service': 'ssl/http', 'version': 'Mongoosehttpd'}, '49152': {'type': 'tcp', 'state': 'open', 'service': 'unknown', 'version': ''}, '49153': {'type': 'tcp', 'state': 'open', 'service': 'unknown', 'version': ''}, '49154': {'type': 'tcp', 'state': 'open', 'service': 'unknown', 'version': ''}, '49155': {'type': 'tcp', 'state': 'open', 'service': 'unknown', 'version': ''}, '49156': {'type': 'tcp', 'state': 'open', 'service': 'unknown', 'version': ''}, '49157': {'type': 'tcp', 'state': 'open', 'service': 'unknown', 'version': ''}, '49158': {'type': 'tcp', 'state': 'open', 'service': 'unknown', 'version': ''}, '49159': {'type': 'tcp', 'state': 'open', 'service': 'unknown', 'version': ''}, '49160': {'type': 'tcp', 'state': 'open', 'service': 'unknown', 'version': ''}, '49161': {'type': 'tcp', 'state': 'open', 'service': 'unknown', 'version': ''}}, 'Filtered': ' 986 filtered tcp ports '}
OS: FreeBSD 11.2-RELEASE
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', 'vpn.av.it.pt': '193.136.92.1'}

CVE-2016-10012

cvss: 7.2
severity: High
cwe: CWE-119
cvss-vector: AV:L/AC:L/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'LOCAL'}
Rating: 7.2

193.136.92.51 - www.mobiwise.nap.av.it.pt

name: www.mobiwise.nap.av.it.pt
ports: {'open': {'25': {'type': 'tcp', 'state': 'open', 'service': 'tcpwrapped', 'version': ''}, '80': {'type': 'tcp', 'state': 'open', 'service': 'http', 'version': 'MicrosoftIIShttpd8.5'}, '135': {'type': 'tcp', 'state': 'open', 'service': 'msrpc', 'version': 'MicrosoftWindowsRPC'}, '443': {'type': 'tcp', 'state': 'open', 'service': 'ssl/http', 'version': 'MicrosoftHTTPAPIhttpd2.0(SSDP/UPnP)'}, '445': {'type': 'tcp', 'state': 'open', 'service': 'microsoft-ds', 'version': 'MicrosoftWindowsServer2008R2-2012microsoft-ds'}, '990': {'type': 'tcp', 'state': 'open', 'service': 'tcpwrapped', 'version': ''}, '49155': {'type': 'tcp', 'state': 'open', 'service': 'msrpc', 'version': 'MicrosoftWindowsRPC'}}, 'Filtered': ' 993 filtered tcp ports '}
OS:
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', 'webserv2.av.it.pt': '193.136.92.51'}

CVE-1999-0488

cvss: 7.5
severity: High
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2000-0122

cvss: 5.0
severity: Medium
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2000-0160

cvss: 7.6
severity: High
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:H/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'HIGH', 'vector': 'NETWORK'}

CVE-2000-0256

cvss: 7.5
severity: High
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2000-0544

cvss: 5.0
severity: Medium
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2002-0419

cvss: 5.0
severity: Medium
cwe: CWE-200
cvss-vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2004-0790

cvss: 5.0
severity: Medium
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2004-0928

cvss: 5.0
severity: Medium
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2004-1060

cvss: 5.0
severity: Medium
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2004-2383

cvss: 5.1
severity: Medium
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:H/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'HIGH', 'vector': 'NETWORK'}

CVE-2005-0563

cvss: 4.3
severity: Medium
cwe: CWE-79
cvss-vector: AV:N/AC:M/Au:N/C:N/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'NONE', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2006-3697

cvss: 7.2
severity: High
cwe: CWE-264
cvss-vector: AV:L/AC:L/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'LOCAL'}

CVE-2006-3942

cvss: 7.8
severity: High
cwe: CWE-20
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2006-5395

cvss: 7.5
severity: High
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2006-6627

cvss: 10.0
severity: Critical
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:L/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2007-0038

cvss: 9.3
severity: Critical
cwe: CWE-119
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2007-1765

cvss: 9.3
severity: Critical
cwe: NVD-CWE-noinfo
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2007-6502

cvss: 5.5
severity: Medium
cwe: CWE-200
cvss-vector: AV:N/AC:L/Au:S/C:P/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'SINGLE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2008-0085

cvss: 5.0
severity: Medium
cwe: CWE-200
cvss-vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2008-0107

cvss: 9.0
severity: Critical
cwe: CWE-189
cvss-vector: AV:N/AC:L/Au:S/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'SINGLE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2008-1447

cvss: 5.0
severity: Medium
cwe: CWE-331
cvss-vector: AV:N/AC:L/Au:N/C:N/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'NONE', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2008-3243

cvss: 4.3
severity: Medium
cwe: CWE-20
cvss-vector: AV:N/AC:M/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2009-0087

cvss: 9.3
severity: Critical
cwe: NVD-CWE-noinfo
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2009-0100

cvss: 9.3
severity: Critical
cwe: CWE-399
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2009-0550

cvss: 9.3
severity: Critical
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2009-0557

cvss: 9.3
severity: Critical
cwe: CWE-94
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2009-0560

cvss: 9.3
severity: Critical
cwe: CWE-399
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2009-0561

cvss: 9.3
severity: Critical
cwe: CWE-189
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2009-0563

cvss: 9.3
severity: Critical
cwe: CWE-119
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2009-0565

cvss: 9.3
severity: Critical
cwe: CWE-119
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2009-1134

cvss: 9.3
severity: Critical
cwe: CWE-94
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2009-2499

cvss: 8.5
severity: High
cwe: CWE-94
cvss-vector: AV:N/AC:M/Au:S/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'SINGLE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2010-1263

cvss: 9.3
severity: Critical
cwe: CWE-94
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2010-1425

cvss: 5.0
severity: Medium
cwe: NVD-CWE-Other
cvss-vector: AV:N/AC:L/Au:N/C:N/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'NONE', 'integrity': 'PARTIAL'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2010-1900

cvss: 9.3
severity: Critical
cwe: CWE-94
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2010-1901

cvss: 9.3
severity: Critical
cwe: CWE-94
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2010-1902

cvss: 9.3
severity: Critical
cwe: CWE-119
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2012-1854

cvss: 6.9
severity: Medium
cwe: NVD-CWE-Other
cvss-vector: AV:L/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'LOCAL'}

CVE-2015-4950

cvss: 4.0
severity: Medium
cwe: CWE-200
cvss-vector: AV:N/AC:L/Au:S/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'SINGLE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2015-6557

cvss: 2.1
severity: Low
cwe: CWE-200
cvss-vector: AV:L/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'LOCAL'}

CVE-2015-7404

cvss: 1.9
severity: Low
cwe: CWE-200
cvss-vector: AV:L/AC:M/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'LOCAL'}

CVE-2017-0098

cvss: 2.9
severity: Low
cwe: CWE-20
cvss-vector: AV:A/AC:M/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'ADJACENT_NETWORK'}

CVE-2018-5282

cvss: 7.2
severity: High
cwe: CWE-787
cvss-vector: AV:L/AC:L/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'LOCAL'}

CVE-2018-5391

cvss: 7.8
severity: High
cwe: CWE-20
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-1000

cvss: 3.5
severity: Low
cwe: CWE-269
cvss-vector: AV:N/AC:M/Au:S/C:N/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'NONE', 'integrity': 'PARTIAL'}
access: {'authentication': 'SINGLE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2019-16863

cvss: 4.3
severity: Medium
cwe: CWE-327
cvss-vector: AV:N/AC:M/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2020-1296

cvss: 2.1
severity: Low
cwe: CWE-200
cvss-vector: AV:L/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'LOCAL'}

CVE-2020-1459

cvss: 2.1
severity: Low
cwe: CWE-200
cvss-vector: AV:L/AC:L/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'LOCAL'}

CVE-2020-26233

cvss: 3.6
severity: Low
cwe: CWE-706
cvss-vector: AV:N/AC:H/Au:S/C:P/I:P/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'PARTIAL'}
access: {'authentication': 'SINGLE', 'complexity': 'HIGH', 'vector': 'NETWORK'}

CVE-2020-35608

cvss: 7.2
severity: High
cwe: CWE-74
cvss-vector: AV:L/AC:L/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'LOCAL'}

CVE-2021-21505

cvss: 10.0
severity: Critical
cwe: CWE-522
cvss-vector: AV:N/AC:L/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2021-38505

cvss: 4.3
severity: Medium
cwe: CWE-668
cvss-vector: AV:N/AC:M/Au:N/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2021-44228

cvss: 9.3
severity: Critical
cwe: CWE-502
cvss-vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}
Rating: 10.0

193.136.92.147 - xcoa.av.it.pt

name: xcoa.av.it.pt
ports: {'open': {'22': {'type': 'tcp', 'state': 'open', 'service': 'ssh', 'version': 'OpenSSH8.2p1Ubuntu4ubuntu0.3(UbuntuLinux;protocol2.0)'}, '80': {'type': 'tcp', 'state': 'open', 'service': 'http', 'version': 'Apachehttpd2.4.41((Ubuntu))'}, '443': {'type': 'tcp', 'state': 'open', 'service': 'ssl/http', 'version': 'Apachehttpd2.4.41((Ubuntu))'}}, 'Filtered': ' 997 closed tcp ports '}
OS:
Route: {'l0703319-ws01.ua.pt': '172.17.0.1', '10.0.12.2': '10.0.12.2', 'xcoa.av.it.pt': '193.136.92.147'}

CVE-2012-0814

cvss: 3.5
severity: Low
cwe: CWE-255
cvss-vector: AV:N/AC:M/Au:S/C:P/I:N/A:N
impact: {'availability': 'NONE', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'SINGLE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}

CVE-2016-10012

cvss: 7.2
severity: High
cwe: CWE-119
cvss-vector: AV:L/AC:L/Au:N/C:C/I:C/A:C
impact: {'availability': 'COMPLETE', 'confidentiality': 'COMPLETE', 'integrity': 'COMPLETE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'LOCAL'}

CVE-2016-10708

cvss: 5.0
severity: Medium
cwe: CWE-476
cvss-vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'NONE', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'LOW', 'vector': 'NETWORK'}

CVE-2019-13115

cvss: 5.8
severity: Medium
cwe: CWE-190
cvss-vector: AV:N/AC:M/Au:N/C:P/I:N/A:P
impact: {'availability': 'PARTIAL', 'confidentiality': 'PARTIAL', 'integrity': 'NONE'}
access: {'authentication': 'NONE', 'complexity': 'MEDIUM', 'vector': 'NETWORK'}
Rating: 7.2