cerca nel menu..

Home
Base Tables
Configurations
Clients
Management
Vulnerability Devices
Imports

Admin Area

Welcome back Gian Luca Borghesan

Directional Dashboard

Customer Filter

Customer

Demo Scudata

Customer Data

Demo Scudata

Strada statale 12 Milano (MI) - Italy

Net: **Demo Network (25-08-2024 11:54)**

IPs Counted: **15**

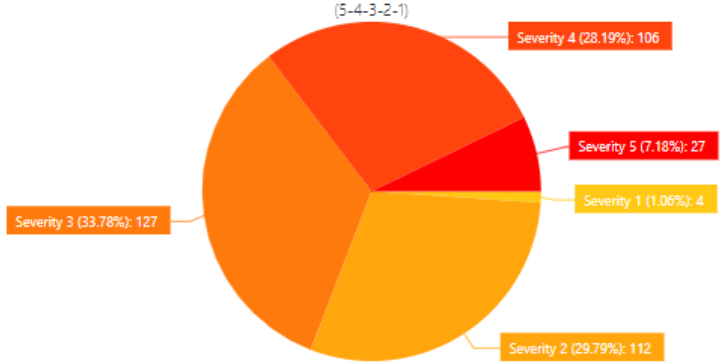
IPs Scanned: **14**

IPs Not Found: **1**

Vulnerabilities Found: **376**

VULNERABILITY TYPE

(5-4-3-2-1)

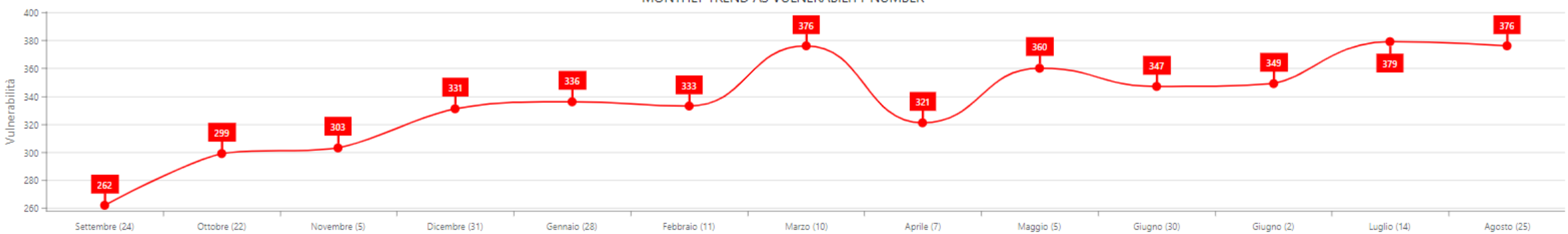


19 Malware

82 Exploit

Potential ransom demanded in case of attack

MONTHLY TREND AS VULNERABILITY NUMBER



Layout di default di Vulnerabilità Dispositivi

Vulnerability Devices

Last Scan

25-08-2024 11:54 - Demo Scudata [Demo Network]

Search Vulnerability Devices

Drag a column header here to group by that column

Generation Date	IP	Track Type	Device Name	Priority	NETBIOS	Operating System	Device Group	Vulner...	V1	V2	V3	V4	V5	Malwa...	Exploit	Quara...
25/08/2024	172.19.1.164	Dns	Portatile Responsabile	High	NBZEN01	Windows 2016/2019/10	Computer	31	0	6	11	12	2	2	3	
25/08/2024	172.19.1.254	IP				EulerOS / Ubuntu / Fedora / Tiny Core Linux / Linux 3.x / IBM / FortiSOAR / F5 Networks Big-IP		18	0	13	3	2	0	0	1	
25/08/2024	172.19.1.15	IP				VMware ESXi 7.0.3 build 23307199		9	0	7	2	0	0	0	0	
25/08/2024	172.19.1.58	IP				Juniper Networks JUNOS / Juniper Router		8	0	8	0	0	0	0	0	
25/08/2024	172.19.1.57	IP				Juniper Networks JUNOS / Juniper Router		6	0	6	0	0	0	0	0	
25/08/2024	172.19.1.21	IP			NAS02	Ubuntu / Tiny Core Linux / Linux 2.6.x		13	0	9	4	0	0	0	3	
25/08/2024	172.19.1.20	Dns			NAS	Linux 2.4-2.6 / Embedded Device / F5 Networks Big-IP / Integrated Management Module / Microsoft CIFS Server		26	1	11	13	1	0	0	7	
25/08/2024	10.2.7.84	Agent			NBZEN01	Windows 11 Pro 64 bit Edition Version 23H2		23	0	5	13	5	0	2	5	
25/08/2024	192.168.1.13	Agent			NB-GIANLUCA	Windows 11 Pro 64 bit Edition Version 23H2		54	1	4	16	19	14	3	19	
25/08/2024	172.19.1.161	Agent			MBPCTEC01	Windows 11 Pro 64 bit Edition Version 23H2		45	1	5	13	24	2	3	13	
25/08/2024	172.19.1.163	Agent			MBTWRK	Windows 11 Pro 64 bit Edition Version 23H2		93	0	11	31	42	9	9	18	
25/08/2024	172.19.1.21	Dns			NAS02	Ubuntu / Tiny Core Linux / Linux 2.6.x		12	0	8	4	0	0	0	3	
25/08/2024	172.19.1.21	Dns			NAS02	Ubuntu / Tiny Core Linux / Linux 2.6.x		12	0	8	4	0	0	0	3	
25/08/2024	172.19.1.20	Dns			NAS	Linux 2.4-2.6 / Embedded Device / F5 Networks Big-IP / Integrated Management Module / Microsoft CIFS Server		26	1	11	13	1	0	0	7	

1 of 1

100

Vulnerabilities 172.19.1.164 - Portatile Responsabile - NBZEN01

Device Data

Demo Scudata

Operating System: Windows 2016/2019/10

Device Group: Computer

Priority: High

Vulnerabilities: **31**

Malware: **2**

Exploit: **3**

Vulnerability Detail

Search Vulnerabilita

Drag a column header here to group by that column

	Key	Vulnerabilities	Severity	Category	Malware	Exploit	Track Type	Gateway	Protocol	SSL	Date First Time	Date Last Time	Amount	Status	Last Correcti... Date
	qid_378791	Zoom Desktop Client Escalation Privilege Vulnerability (ZSB-23032)	Severity 5	Local	☐	☐	Dns	0		☐	28/08/2...	27/10/2...	13	Active	
	qid_378778	Zoom Desktop Client Path Traversal Vulnerability (ZSB-23030)	Severity 5	Local	☐	☐	Dns	0		☐	28/08/2...	27/10/2...	13	Active	
	qid_375518	OpenVpn 2.5.1 and earlier Authentication Bypass (excluding 2.4.11)	Severity 4	Local	☐	☐	Dns	0		☐	14/04/2...	27/10/2...	46	Active	
	qid_378332	Microsoft WinVerifyTrust Signature Validation Vulnerability	Severity 4	Local	☑	☑	Dns	0		☐	23/05/2...	27/10/2...	30	Active	
	qid_378814	Zoom Client Exposure of Sensitive Information Vulnerability (ZSB-23039)	Severity 4	Local	☐	☐	Dns	0		☐	01/09/2...	27/10/2...	12	Active	
	qid_378785	Zoom Desktop Client Escalation Privilege Vulnerability (ZSB-23027)	Severity 4	Local	☐	☐	Dns	0		☐	28/08/2...	27/10/2...	13	Active	
	qid_378783	Zoom Desktop Client Information Disclosure Vulnerability (ZSB-23041, ZSB-23036)	Severity 4	Local	☐	☐	Dns	0		☐	28/08/2...	27/10/2...	13	Active	
	qid_378780	Zoom Client, VDI Escalation Privilege Vulnerability (ZSB-23038)	Severity 4	Local	☐	☐	Dns	0		☐	28/08/2...	27/10/2...	13	Active	
	qid_378717	Zoom Client Improper Input Validation Vulnerability (ZSB-23018)	Severity 4	Local	☐	☐	Dns	0		☐	28/08/2...	27/10/2...	13	Active	
	qid_92053	Microsoft Windows Defender Elevation of Privilege Vulnerability for August 2023	Severity 4	Windows	☐	☐	Dns	0		☐	28/08/2...	27/10/2...	13	Active	
	qid_378790	WinRAR Multiple Remote Code Execution (RCE) Vulnerabilities	Severity 4	Local	☑	☑	Dns	0		☐	28/08/2...	27/10/2...	13	Active	

Microsoft WinVerifyTrust Signature Validation Vulnerability

Vulnerabilities

Severity:

Severity 4

Category:

Local

Malware:

Exploit:

Threat:

Microsoft stated that they have re-published the CVE-2013-3900 to inform customers about the availability of EnableCertPaddingCheck. This behavior remains available as an opt-in feature via the registry key setting and is available on all supported editions of Windows released since December 10, 2013.
Microsoft recommends that executable authors consider conforming all signed binaries to the new verification standard by ensuring that they contain no extraneous information in the WIN_CERTIFICATE structure.
Microsoft also recommends that customers appropriately test this change to evaluate how it will behave in their environments.

Microsoft recommends that customers test how this change to Authenticode signature verification behaves in their environment before fully implementing it. To enable the Authenticode signature verification improvements, modify the registry to add the EnableCertPaddingCheck value as detailed below.
- HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\Wintrust\Config "EnableCertPaddingCheck"="1"
- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Cryptography\Wintrust\Config "EnableCertPaddingCheck"="1"

QID Detection Logic (Authenticated):
This QID checks for the presence of these registry keys HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\Wintrust\Config and HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Cryptography\Wintrust\Config, and checks whether the value 'EnableCertPaddingCheck' associated with these keys is set to 1 (REG_SZ).
If these keys are missing or the value is not set to 1 or if the type of registry value EnableCertPaddingCheck is not REG_SZ (string), then this QID gets reported.

Impact:

A remote code execution vulnerability exists in the way that the WinVerifyTrust function handles Windows Authenticode signature verification for portable executable (PE) files. An anonymous attacker could exploit the vulnerability by modifying an existing signed executable file to leverage unverified portions of the file in such a way as to add malicious code to the file without invalidating the signature.

Solution:

Customers are advised to refer to WinVerifyTrust Signature Validation for further details pertaining to this.
Opting into this stricter verification behavior causes the WinVerifyTrust function to perform strict Windows Authenticode signature verification for PE files. After opting-in, PE files will be considered "unsigned" if Windows identifies content in them that does not conform to the Authenticode specification. This may impact some installers. If you are using an installer that is impacted, Microsoft recommends using an installer that only extracts content from validated portions of the signed file.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

CVE-2013-3900

SCUDATA
cyber security

Gian Luca Borghesan
Socio Fondatore e Presidente
Cyber Security Specialist

Phone: +39 059 8678833
Mobile: +39 393 750 1998
Email: g.borghesan@scudata.it

https://www.scudata.it/