

Incident Handling - Tags

[[Allgemeines](#)] [[Die Tags](#)]

Incident Handling: Tags für automatische Securityhinweise

Allgemeines

Das ACONet-CERT interpretiert Beobachtungen, die selbst gemacht (z.B. durch Auswertung von Netzstatistiken) oder von anderen Organisationen (CERTs, Security-Teams, etc...) übermittelt werden in einem weitgehend automatisierten Prozess. Ergibt die Auswertung eine hinreichende Wahrscheinlichkeit für ein Sicherheitsproblem, werden die vorhandenen Informationen als Securityhinweise an die jeweiligen ACONet-Teilnehmer weitergeleitet.

⚠ Securityhinweise sind stets das Ergebnis der Interpretation von Beobachtungen und können Irrtümer enthalten.

Die meisten Problemhinweise mit einem **Tag** bezeichnet. Genauere Beschreibungen und Hintergrundinformationen dazu können über die folgende Liste abgerufen werden. **Tags** bestehen aus zwei oder drei Teilen, die jeweils durch einen Punkt verbunden sind, beginnend mit der Kategorie:

Attack

Der betreffende Rechner nimmt an DoS-Angriffen teil, versucht in Systeme einzudringen (Exploits, Brute Force-Angriffe) oder zeigt ein Verhalten, das einen bevorstehenden Angriff vermuten lässt.

Bot

Der betreffende Rechner nimmt an einem Botnet teil. Dieser Alarm wird zumeist durch die (versuchte) Kontaktaufnahme mit einem Command&Control-Servern ausgelöst.

Spam

Versand von Spam (Blacklisten, Spamtraps...) oder für Malware, die Spam oder infizierte Mail versendet. Auch bei gesperrtem SMTP-Port kann es zu Hinweisen aus dieser Kategorie kommen: Webmail, webbasierten Medien wie Blogs und Foren, Kontakt mit Command&Control-Servern.

Compromised

Sammelkategorie für unsichere Zustände eines Rechners, die nicht genauer mit einer der obigen Kategorien beschrieben werden können: Rechner ist von Malware befallen, ein Account ist gehackt worden, etc...

Phishing

Phishing-Webseiten oder anders in Phishing-Aktivitäten involvierte Adressen.

Vulnerability

Schwachstellen, soweit sie dem ACONet-CERT durch Hinweise von außen oder durch eigene Tests bekannt werden. Die Kategorie Vulnerability kann und soll keineswegs Pentests oder Security-Scans ersetzen, vielmehr werden ausgewählte Problemfelder behandelt. Auf eine Klasse von Vulnerabilities, die UDP-basiert DoS-Angriffe ermöglichen, wird im Dokument [Amplified UDP reflection attack](#) näher eingegangen.

Die Tags

Tag	Kurzbeschreibung
Attack.Portscan	Rechner führt Portscans durch (viele Zielports und/oder viele Zieladressen)
Attack.Sony.com	Geräte versuchen die Dienste von SONY zu beeinträchtigen oder Accounts von SONY Kunden zu kompromittieren.
Bot.CBL	Rechner ist auf der CBL-Blacklist verzeichnet
Bot.Conficker.C&C	Kontakt mit einem C&C-Server des Conficker-Botnets
Bot.Rustock.C&C	Kontakt mit einem von Microsoft + Security-Firmen übernommenen Rustock-C&C-Server
Bot.Torpig_Mebroot.C&C	Kontakt mit einem C&C-Server des Torpig/Mebroot-Botnets
Compromised.Account	Geheimnisverlust von Username & Passwort / sonstigen Credentials

Compromised.Harvester.project_honeypot	Rechner sucht nach Mailadressen, an die Spam gesendet wird
Phishing.phishtank_org	Phishing-Webseiten, die bei Phishtank.org gemeldet wurden.
Spam.Blacklist.NIXSPAM	Rechner ist auf der NIXSPAM-Blacklist verzeichnet
Spam.Blacklist.PSBL	Rechner ist auf der PSBL-Blacklist verzeichnet
Spam.Blacklist.QUORUM_TO	Rechner ist auf der QUORUM.TO-Blacklist verzeichnet
Spam.Blacklist.SpamCop	Rechner ist auf der SpamCop-Blacklist verzeichnet
Spam.Blacklist.UCEPROTECT	Rechner ist auf der UCEPROTECT1-Blacklist verzeichnet
Spam.Web.project_honeypot	Spam in Webforen, Blogs, etc.
Spam.postmaster_live_com	Spamhost-Informationen von postmaster.live.com (Hotmail)
Spam.Spamtrap	Header oder Auszüge von Nachrichten, die an Spamtrapadressen geschickt wurden
Vuln.amt	Authentication Bypass bei AMT-Fernwartungsfunktionalität – CVE-2017-5689
Vuln.ntpd_peerlist	Time-Server, der mittels peerlist-Befehl für DoS-Angriffe mißbraucht werden kann
Vuln.ntpd_monlist	Time-Server, der mittels monlist-Befehl für DoS-Angriffe mißbraucht werden kann
Vuln.open_recurser	Ungeschützter Nameserver, der für DoS-Angriffe mißbraucht werden kann
Vuln.open_chargen	Ungeschützter Chargen-Server, der für DoS-Angriffe mißbraucht werden kann
Vuln.openssl_heartbeat	OpenSSL-Verwundbarkeit "Heartbleed" – CVE-2014-0160
Vuln.open_snmp	Ungeschützte SNMP-Server, die für DoS-Angriffe mißbraucht werden können
Vuln.weak_cipher	Server unterstützt veraltete Verschlüsselungsmethoden
Vuln.open_portmapper	Ungeschütztes Portmapper Service, das für DoS-Angriffe missbraucht werden kann