RISKSENSE

CVEs associated with Ryuk Ransomware family

(Last updated 20201001)

SNO	CVE Id	Vendor & Product	Known Exploits	APT Group	CVSSv2	CVSSv3	Patch
1	CVE-2018-8389	Microsoft, Internet Explorer			7.6	7.5	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8389
2	CVE-2013-2618	Network-weathermap, .network Weathermap			4.3		http://www.network-weathermap.com/content/security-notice-cve-2013-2618-network-weathermap-097a-persistent-xss
3	CVE-2017-6884	Zyxel, Emg2926 Firmware			9		https://www.exploit-db.com/exploits/41782/
4	CVE-2018-12808	Adobe, Acrobat DC, Acrobat Reader DC			7.5	9.8	https://helpx.adobe.com/security/products/acrobat/apsb18-29.html
5	CVE-2017-0143	Microsoft, Server Message block	Eternal blue	APT3, Calypso	9.3	8.1	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0143
6	CVE-2017-0144	Microsoft, Server Message block	Eternal blue	Lazarus Group (APT37& APT38)	9.3	8.1	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0144

7	CVE-2017-0145	Microsoft, Server Message block		Lazarus Group (APT37& APT38)	9.3	8.1	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0145
8	CVE-2017-0146	Microsoft, Server Message block		Shadow Brokers	9.3	8.1	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0146
9	CVE-2017-0147	Microsoft, Server Message block		Shadow Brokers	4.3	5.9	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0147
10	CVE-2019-6109	Canonical Debian Netapp Openbsd Winscp Ubuntu Linux Debian Linux Element software Ontap Select deploy Openssh Winscp Storage Automation Store			4	6.8	https://cvsweb.openbsd.org/src/usr.bin/ssh/progressmeter.c
11	CVE-2019-6110	Netapp Openbsd, Winscp Openssh Storage Automation Store Ontap Select Deploy			4	6.8	https://cvsweb.openbsd.org/src/usr.bin/ssh/scp.c

		Element Software					
12	CVE-2019-6111	Canonical Debian Redhat Openbsd Winscp Winscp Openssh Enterprise Linux Debian Linux Ubuntu Linux			5.8	5.9	https://security.netapp.com/advisory/ntap-20190213-0001/
13	CVE-2018-20685	Canonical Debian Redhat Openbsd Winscp Netapp Oracle Ubuntu Linux Debian Linux Element software Ontap Select deploy Openssh Winscp Storage Automation Store Cloud Backup Solaris Enterprise Linux			2.6	5.3	https://cvsweb.openbsd.org/cgi-bin/cvsweb/src/usr.bin/ssh/scp.c.diff?r1=1.197&r2=1.198&f=h

Ryuk MITRE ATT&CK

ATT&CK Tactic Category	Techniques
Privilege Escalation	T1134 - Access Token Manipulation
Persistence	T1547 - Boot or Logon Autostart Execution: Registry Run Keys /Startup Folder T1059 - Command and Scripting Interpreter: Windows Command Shell
Impact	T1486 - Data Encrypted for Impact T1490 - Inhibit System Recovery T1489 - Service Stop
Discovery	T1083 - File and Directory Discovery T1057 - Process Discovery T1016 - System Network Configuration Discovery
Defense Evasion	T1562 - Impair Defenses: Disable or Modify Tools T1036 - Masquerading: Match Legitimate Name or Location T1055 - Process Injection
Execution	T1106 - Native API

About RiskSense

RiskSense®, Inc. provides full-spectrum vulnerability management and prioritization to measure and control cybersecurity risk across infrastructure and applications. The cloud-based RiskSense platform uses a foundation of risk-based scoring, analytics, and technology-accelerated pen testing to identify critical security weaknesses with corresponding remediation action plans, dramatically improving the efficiency and effectiveness of Security, Development, and IT. For more information, visit www.risksense.com or follow us on Twitter at @RiskSense.