UBND TỈNH QUẢNG NINH
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập – Tự do – Hạnh phúc

Số: 417/STTTT - CNTT
Vv cảnh báo nguy cơ tấn công vào các máy chủ web sử dụng Apache Tomcat.

Quảng Ninh, ngày 13 tháng 3 năm 2020

Kính gửi:

- Văn phòng Tỉnh ủy;
- Văn phòng Đoàn ĐBQH, HĐND và UBND tỉnh;
- Các Sở, ban, ngành, đoàn thể tỉnh;
- UBND các huyện, thị xã, thành phố.

Sở Thông tin và Truyền thông nhận được công văn số 135/CATTT-NCSC ngày 09/3/2020 của Cục An toàn thông tin về cảnh báo nguy cơ tấn công vào các máy chủ web sử dụng Apache Tomcat, theo đó, Ngày 21/02/2020, Hệ thống Cảnh báo điểm yếu và rà soát lỗ hổng bảo mật tự động của Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), Cục An toàn thông tin đã ghi nhận lỗ hổng CVE-2020-1938 (còn gọi là Ghostcat) trong thành phần Apache JServ Protocol của các máy chủ web sử dụng Apache Tomcat. Lỗ hổng này ảnh hưởng tới nhiều phiên bản Tomcat (Tomcat 9/8/7/6 và các phiên bản cũ hơn) và đã có mã khai thác công khai trên Internet.

Thông qua khai thác lỗ hổng trên, đối tượng tấn công có thể thu thập thông tin nội dung các tệp trên máy chủ Tomcat bao gồm cả tập tin cấu hình. Ngoài ra, nếu ứng dụng web cho phép người dùng tải tệp lên, thì đối tượng tấn công có thể lợi dụng để tải lên máy chủ các đoạn mã khai thác và thực thi nhiều hành động độc hại khác. Qua đánh giá sơ bộ, Việt Nam có khoảng 3.313 máy chủ web có sử dụng Apache Tomcat đang công khai trên Internet. Những máy chủ này hầu hết chưa được cập nhật bản vá và sẽ là những hệ thống đầu tiên đối tượng tấn công nhằm đến.

Nhằm bảo đảm an toàn thông tin và phòng tránh việc đối tượng tấn công lợi dụng điểm yếu an toàn thông tin để thực hiện những cuộc tấn công mạng nguy hiểm, Sở Thông tin và Truyền thông đề nghị các cơ quan, đơn vị, địa phương, các quản trị mạng và người dùng thực hiện:

1. Rà soát các máy chủ Apache Tomcat để phát hiện và xử lý kịp thời các máy chủ có khả năng đã bị đối tượng tấn công khai thác thông qua lỗ hổng trên. Danh sách phiên bản Tomcat bị ảnh hưởng tại Phụ lục 1.

2. Vá lỗ hổng CVE-2020-1938, theo cách sau vô hiệu hoá thành phần lỗi, hoặc nâng cấp lên phiên bản Apache Tomcat mới. Các phiên bản Apache Tomcat đã được khắc phục lỗi cho từng phiên bản đã có trên https://tomcat.apache.org.

3. Tăng cường theo dõi giám sát hệ thống đồng thời thường xuyên theo dõi kênh cảnh báo của các cơ quan chức năng và các tổ chức lớn về an toàn để phát hiện kịp thời các nguy cơ tấn công mạng.

Trong trường hợp cần thiết, đề nghị cơ quan, đơn vị, cá nhân liên hệ để được phối hợp hỗ trợ, xử lý:

-Trung tâm Công nghệ thông tin và Truyền thông, Sở Thông tin và Truyền thông, điện thoại: 0203 3533338, email:qnict@quangninh.gov.vn.

- Trung tâm Giám sát an toàn không gian mạng quốc gia thuộc Cục An toàn thông tin, điện thoại: 024.3209.1616, email ais@mic.gov.vn

Trân trọng./.

Nơi nhận:
- Như trên;
- UBND tỉnh (B/c);
- Cục ATTT (B/c);
- Đ/c GĐ Sở (B/c);
- Các đ/c PGĐ Sở;
- Trung tâm GSATKGM quốc gia (p/h);
- Trung tâm CNTT&TT (t/h);
- Lưu: VT, CNTT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

Đinh Sỹ Nguyên

PHỤ LỤC 1

Danh sách phiên bản Tomcat bị ảnh hưởng

(kèm theo Công văn số 417/STTTT-CNTT ngày 13/3/2020)

Phiên bản	Phiên bản đã khắc phục lỗi Apache
Tomcat 9 (9.x < 9.0.31)	9.0.31
Apache Tomcat 8 (8.x < 8.5.51)	8.5.51
Apache Tomcat 7 (7.x < 7.0.100)	7.0.100

PHỤ LỤC 2

Danh sách một số máy có thể bị ảnh hưởng bởi CVE-2020-1938

(kèm theo Công văn số 417/STTTT-CNTT ngày 13/3/2020)

STT	IP	Cổng	Tên tổ chức/ISP
1	125.212.193.81	8009	Công ty Cổ phần Chứng khoán VNDirect
2	103.196.236.102	8083	Trung tâm Internet Việt Nam VNNIC
3	117.103.197.134	8081	Tổng Công ty Truyền thông Đa phương tiện VN (VTC)
4	117.103.205.123	8181	
5	113.160.172.195	8081	
6	61.28.235.233	8080	Công ty CP Công nghệ Sao Bắc Đẩu
7	221.133.26.65	80	Công ty CP DV Bưu chính Viễn thông Sài Gòn
8	118.69.52.88	8081	
9	118.69.218.82	80	Công ty CP Giải Pháp Hệ Thống Long Vân
10	103.92.26.32	8081	
11	103.74.121.143	8880	Công ty CP giải pháp mạng Bạch Kim
12	117.2.128.11	8880	Công ty CP VCCorp
13	45.119.81.170	8081	Công ty phần mềm Quang Trung
14	14.160.24.29	8181	Công ty TNHH Thương mại Dịch vụ Quảng cáo ảo Hóa Việt
15	45.122.223.23	8081	Công ty TNHH TM Dịch vụ Giải pháp Việt
16	103.56.156.244	9001	Công ty TNHH TM Soha
17	113.161.116.43	8080	Công ty TNHH Viễn Thông Minh Tú
18	103.90.225.121	8081	Công ty TNHH Vietnix Cloud
19	120.72.110.135	443	
20	124.158.6.61	8081	Công ty TNHH Viettel (CHT)
21	118.69.70.215	8081	
22	123.39.240.28	8880	Tập đoàn Bưu chính Viễn thông (VNPT)
23	203.210.192.142	8011	
24	113.161.145.181	8081	
25	118.70.186.154	8081	
26	123.31.31.73	8081	
27	14.225.5.242	8081	
28	222.254.35.8	8081	
29	222.254.35.12	8081	
30	14.177.152.93	8081	
31	117.103.205.124	8181	
32	113.174.246.2	8880	
33	113.190.233.10	8081	

34	14.161.21.69	8880	
35	113.161.75.60	9090	
36	14.169.62.115	8081	
37	113.176.121.37	8081	
38	203.113.135.29	8880	
39	103.69.193.17	9001	
40	123.30.19.14	80	
41	222.254.35.10	8011	
42	14.177.147.6	8011	
43	14.162.208.70	8011	
44	171.244.38.144	8083	
45	113.161.213.241	8181	
46	14.161.35.121	8080	
47	123.30.19.19	80	
48	113.160.248.139	8880	
49	123.16.176.41	8081	
50	113.161.212.209	8181	
51	113.163.94.8	8081	
52	103.53.231.69	8081	
53	124.158.11.243	8880	
54	42.117.236.91	8181	
55	103.90.225.124	8081	
56	14.160.70.2	8081	
57	124.158.6.44	8880	
58	113.161.7.22	8080	
59	117.4.237.115	8080	
60	113.190.253.213	8080	
61	103.31.126.157	9000	
62	113.160.150.89	8880	
63	14.160.24.128	8081	
64	222.252.194.241	8880	
65	210.211.122.65	8083	
66	222.252.14.166	8081	
67	113.161.76.182	8081	
68	113.185.0.250	443	
69	210.245.32.23	8181	
70	112.109.91.210	80	
71	113.161.116.43	443	
72	123.30.23.178	8081	
73	103.31.127.65	8083	

74	115.79.36.222	8081	
75	115.79.203.189	8081	
76	14.241.168.193	8081	
77	124.158.11.55	8080	
78	202.160.125.7	80	Tập đoàn Công nghệ – Viễn thông Quân đội (Viettel)
79	27.72.57.84	8080	
80	113.160.117.38	8081	
81	42.117.236.91	8009	
82	203.162.127.220	8081	
83	117.2.128.10	8880	
84	123.30.19.14	443	
85	118.69.108.78	8181	
86	125.212.252.46	8181	
87	123.30.176.62	8080	
88	210.245.99.225	80	
89	221.133.26.66	80	
90	14.162.18.180	8081	
91	113.161.75.60	8080	
92	124.158.4.235	8081	Tập đoàn Công nghệ CMC
93	42.117.161.81	8081	
94	14.241.75.17	8081	
95	113.161.213.236	8181	
96	210.211.122.63	8080	
97	123.31.12.54	8081	
98	103.92.31.178	8081	
99	118.70.129.16	8880	Công ty Cổ phần Viễn thông FPT
100	118.70.186.154	8081	