BẢO HIỂM XÃ HỘI VIỆT NAM
TRUNG TÂM CÔNG NGHỆ THÔNG TIN

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Số: 271 /BC-CNTT

Hà Nội, ngày 25 *tháng* 02 *năm 2022*

BÁO CÁO KỸ THUẬT
Tình hình an toàn thông tin tháng 01/2022 của các đơn vị trực thuộc Bảo hiểm xã hội Việt Nam và Bảo hiểm xã hội các tỉnh, thành phố trực thuộc Trung ương

1. Thông tin cảnh báo về các lỗ hổng bảo mật

Trung tâm Công nghệ thông tin (CNTT) đã ghi nhận, tổng hợp các cảnh báo an toàn thông tin, lỗ hổng bảo mật từ các đơn vị chuyên trách về an toàn thông tin như sau:

- Công văn số 380/TB-BCA-A05 của Bộ Công An ngày 05/01/2022 thông báo về việc ngăn chặn hoạt động tấn công mạng, khai thác lỗ hổng bảo mật trên Apache Log4j va Apache HTTP. Theo đó, lỗ hổng Apache Log4shell cho phép tin tặc thực thi lệnh điều khiển từ xa, chiếm quyền quản trị, tấn công từ chối dịch vụ máy chủ web; lỗ hổng bảo mật trên Apache HTTP cho phép tin tặc chiếm quyền quản trị từ xa máy chủ, kiểm soát, đánh cắp thông tin, dữ liệu hoặc thực hiện tấn công từ chối dịch vụ. Trung tâm CNTT đã hỗ trợ các đơn vị thiết lập, cập nhật dấu hiệu phát hiện, ngăn chặn hoạt động tấn công, khai thác lỗ hổng, xâm nhập trái phép trên hệ thống mạng trên hệ thống giám sát, tường lửa, thiết bị phòng, chống tấn công mạng và có Công văn số 2644/CNTT-HTA ngày 28/12/2021 về việc rà soát, xử lý lỗ hổng bảo mật trong Apache Log4j ảnh hưởng nghiêm trọng để hướng dẫn các đơn vị rà soát, xác định và khắc phục lỗ hổng.

- Công văn số 56/CATTT-NCSC của Cục An toàn thông tin - Bộ Thông tin và Truyền thông ngày 13/01/2022 về việc lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 01/2022. Theo đó, Microsoft đã phát hành danh sách bản vá tháng 01 ngày 11/01/2022 với 96 lỗ hổng bảo mật trong các sản phẩm của mình trong đó chú ý lỗ hổng CVE-2022-21857 trong Active Directory cho phép đối tượng nâng cao đặc quyền; lỗ hổng bảo mật CVE-2022-21911 trong .NET Framework cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ; lỗ hổng bảo mật CVE-2022-21836 trong Windows Certificate cho phép đối tượng tấn công giả mạo. Trung tâm CNTT đã có Công văn số 75/CNTT-HTA ngày 17/01/2022 về việc xử lý lỗ hổng bảo mật trong các sản phẩm Microsoft công bố tháng 01/2022 để hướng dẫn các đơn vị thực hiện rà soát và cập nhật bản vá lỗ hổng.

Đề nghị phòng CNTT và bộ phận chuyên trách về ứng cứu sự cố tại các đơn vị thực hiện kiểm tra, rà soát, xác định và cập nhật bản vá bảo đảm công tác an toàn thông tin theo quy định; Thường xuyên theo dõi trên hệ thống mạng trên hệ

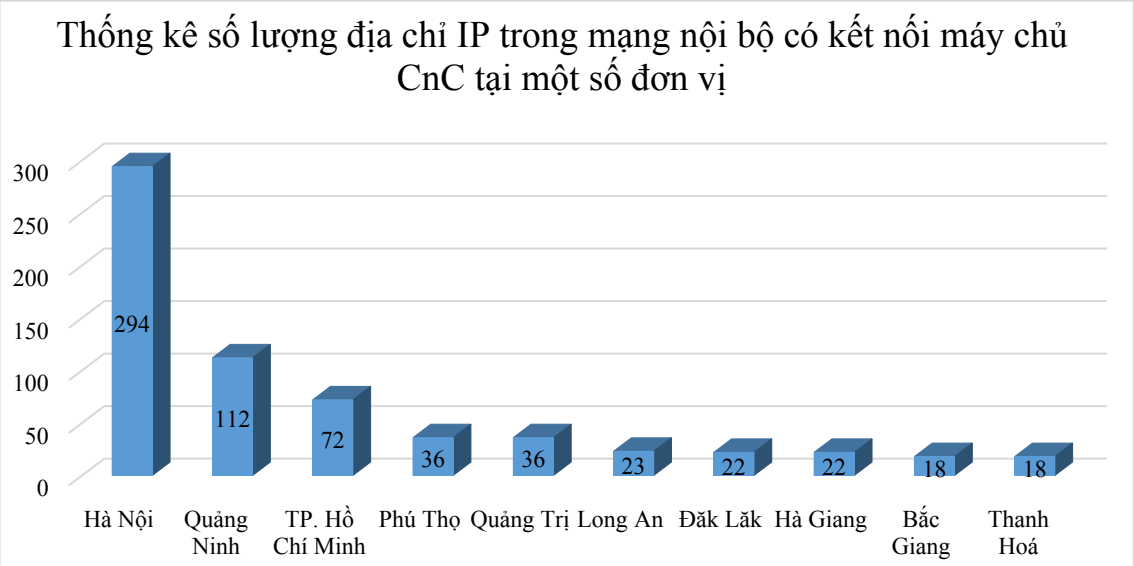
thống giám sát, tường lửa, thiết bị phòng, chống tấn công mạng để kịp thời ngăn chặn hoạt động tấn công mạng, khai thác lỗ hổng bảo mật.

2. Tình hình lây nhiễm mã độc

Hệ thống giám sát của Trung tâm điều hành hệ thống thông tin Ngành BHXH Việt Nam đã ghi nhận 1.228 IP của các đơn vị trực thuộc BHXH Việt Nam và BHXH các tỉnh, thành phố (sau đây gọi chung là các đơn vị) nằm trong mạng botnet, trong đó thông tin giám sát trực tiếp 1.161 địa chỉ IP, thông tin giám sát gián tiếp 67 địa chỉ IP.

2.1. Thông tin giám sát trực tiếp

a) Thông tin kết nối máy chủ điều khiển mã độc (CnC)

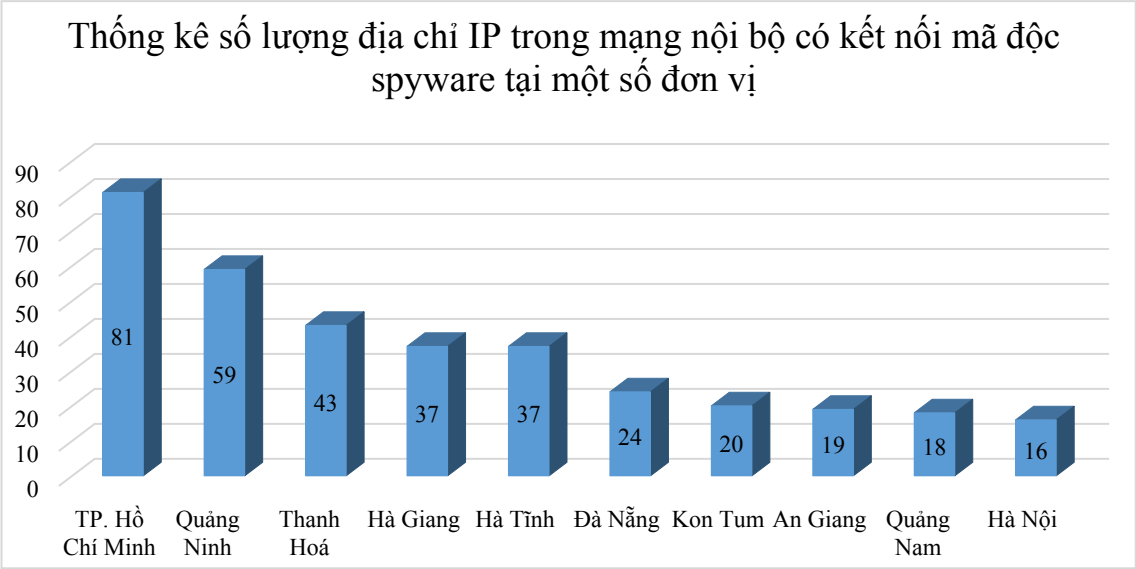


BHXH tỉnh, thành phố: Hà Nội, Quảng Ninh, TP. Hồ Chí Minh, Phú Thọ, Quảng Trị, Long An, Đắk Lắk, Hà Giang, Bắc Giang, Thanh Hóa là những đơn vị có nhiều địa chỉ IP trong mạng nội bộ kết nối đến các máy chủ CnC. Chi tiết các đơn vị có địa chỉ IP kết nối máy chủ CnC tại Phụ lục 1.

b) Thông tin kết nối spyware, virus

Hệ thống tường lửa được BHXH Việt Nam trang bị tại BHXH các tỉnh, thành phố đã ghi nhận 683 địa chỉ IP[1] trong mạng nội bộ của các đơn vị có kết nối mã độc spyware, virus.

[1] Thông tin chi tiết về các địa chỉ IP nội bộ kết nối mã độc spyware, virus các đơn vị tra cứu trên thiết bị tường lửa biên PaloAlto.



BHXH các tỉnh, thành phố: TP. Hồ Chí Minh, Quảng Ninh, Thanh Hóa, Hà Giang, Hà Tĩnh, Đà Nẵng, Kon Tum, An Giang, Quảng Nam, Hà Nội có nhiều địa chỉ IP kết nối đến mã độc spyware. Danh sách đơn vị có địa chỉ IP nội bộ kết nối mã độc spyware, virus tại Phụ lục 2.

2.2. Thông tin giám sát gián tiếp

BHXH tỉnh, thành phố: TP. Hồ Chí Minh, Nam Định có địa chỉ IP public[2] có tình trạng bị rà quét hệ thống.

STT	Địa chỉ IP	Tỉnh	Loại sự cố	Mức độ
8	210.245.33.136	TP. Hồ Chí Minh	event4_sinkhole_http	Nghiêm trọng
9	117.7.236.37	Nam Định	event4_sinkhole_http	Nghiêm trọng

- event4_sinkhole_http: Mã độc được cài đặt trên máy trạm trong hệ thống mạng nội bộ của đơn vị, các ip nhiễm mã độc thuộc mạng botnet HTTP Drone.

- Cách xử lý: Sử dụng phần mềm diệt virus quét sâu đối với các máy tính bị lây nhiễm mã độc, dùng bộ công cụ của Microsoft bóc tách các tiến trình đang nhiễm mã độc theo các bước đã được tập huấn tại diễn tập ứng cứu sự cố an toàn thông tin do Ngành tổ chức.

2.3. Thông tin mã độc được phát hiện, xử lý tại các hệ thống phòng, chống mã độc của Ngành

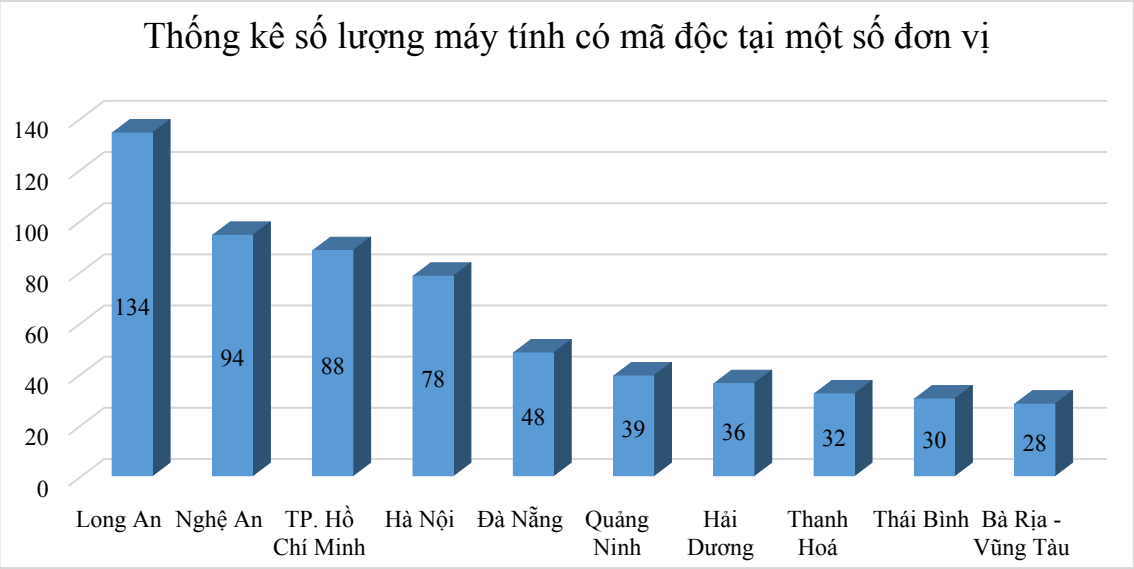
Ngành BHXH Việt Nam đã triển khai các giải pháp phòng, chống phần mềm độc hại (phần mềm diệt virus; phần mềm phát hiện và phản ứng với các cuộc tấn công chưa biết - EDR) để nâng cao năng lực bảo vệ cho máy tính người dùng cuối.

a) Thông tin mã độc được phát hiện

Hệ thống phần mềm diệt virus được Ngành trang bị đã phát hiện tổng số 1.105 máy tính bị nhiễm mã độc, phát hiện 607 loại mã độc đã lây nhiễm trong hệ

[2] Thông tin địa chỉ IP public của các đơn vị được cung cấp cho Trung tâm CNTT để giám sát, trường hợp có thay đổi địa chỉ IP public cần thông báo Trung tâm CNTT bổ sung, cập nhật.

thống máy tính toàn Ngành. Để hệ thống phần mềm diệt virus hoạt động hiệu quả, đưa ra các cảnh báo kịp thời về tình hình lây nhiễm virus trên máy tính cho người dùng đề nghị các đơn vị thường xuyên kiểm tra, bật tính năng quét thời gian thực (real-time scanning) trên hệ thống phần mềm diệt virus.



BHXH tỉnh, thành phố: Long An, Nghệ An, TP. Hồ Chí Minh, Hà Nội, Đà Nẵng, Quảng Ninh, Hải Dương, Thanh Hóa, Thái Bình, Bà Rịa – Vũng Tàu có nhiều máy tính nhiễm mã độc. Thông tin tổng hợp, đánh giá tình hình lây nhiễm mã độc của các đơn vị trên hệ thống quản trị tập trung tại Phụ lục 3.

b) Thông tin cảnh báo EDR

Hệ thống quản trị tập trung phần mềm phát hiện và phản ứng với cuộc tấn công chưa biết (EDR) ngành BHXH Việt Nam đã thống kê có 271.217 lượt cảnh báo tiến trình mã độc MD5/SHA256 (BHXH tỉnh, thành phố: Lạng Sơn, Phú Thọ, Quảng Ninh, Phú Yên...). Trong đó có 56 máy tính người dùng tại các đơn vị chạy tiến trình bị cảnh báo nghi ngờ mã độc, 29 mẫu tiến trình nghi ngờ mã độc được ghi nhận; 163 cảnh báo máy tính thuộc các đơn vị kết nối đến domain độc hại, lừa đảo (BHXH tỉnh, thành phố: Thanh Hóa, Lạng Sơn, Phú Thọ, Hải Dương...); 50 máy tính người dùng nghi ngờ kết nối đến domain độc hại, lừa đảo; 44 domain độc hại, lừa đảo được phát hiện.

Thông tin chi tiết máy tính tại các đơn vị chạy tiến trình chứa mã độc và kết nối đến domail độc hại/lừa đảo được tổng hợp từ hệ thống quản trị tập trung tại Phụ lục 4. Đề nghị các đơn vị rà soát, xử lý đảm bảo an toàn thông tin đồng thời kiểm tra cài đặt lại phần mềm cho những máy tính bị mất kết nối để bảo đảm việc phát hiện và cảnh báo sớm những máy tính có nguy cơ mất ATTT.

2.4. Thông tin rò quét, tấn công thư điện tử

Hệ thống tường lửa chống virus được phát tán qua thư điện tử của Ngành đã ghi nhận, ngăn chặn số lượng lớn thư điện tử phát hiện có virus: 134 thư điện tử có virus trên tầng application; 128.887 | 372 (vào | ra) thư điện tử bị nghi ngờ là thư rác được ngăn chặn và cảnh báo đến người dùng; 187 thư điện tử đính kèm link giả mạo với mục đích đánh cắp mật khẩu của người dùng; 01 tài khoản thư

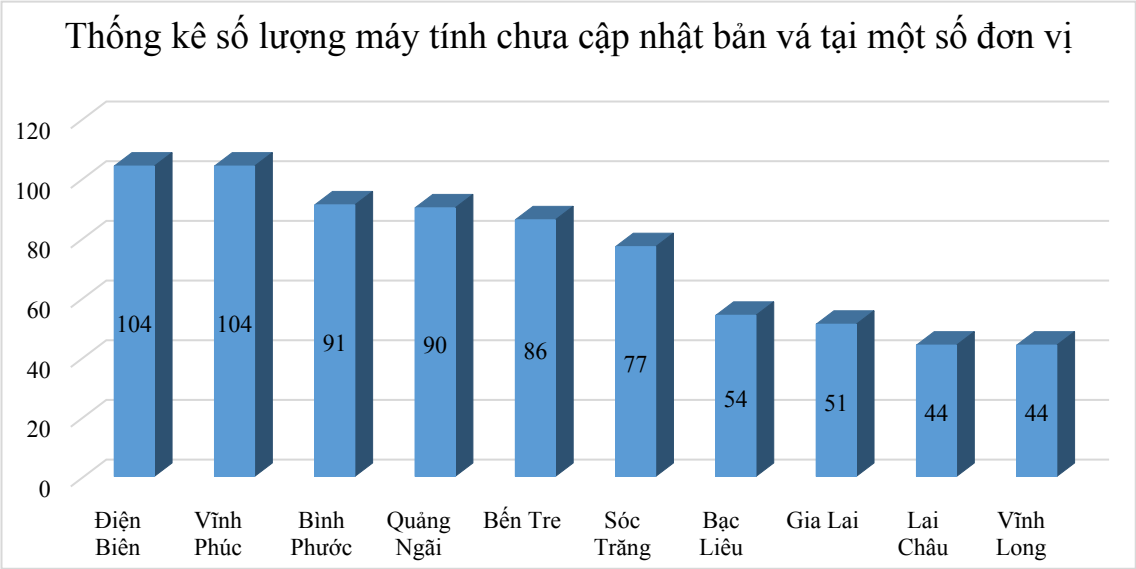
điện tử người dùng thuộc BHXH tỉnh Hà Nam lộ lọt mật khẩu: khuongdtm@hanam.vss.gov.vn.

Đề nghị các đơn vị yêu cầu các cá nhân thay đổi mật khẩu tài khoản và thực hiện nghiêm quy định sử dụng thư điện tử.

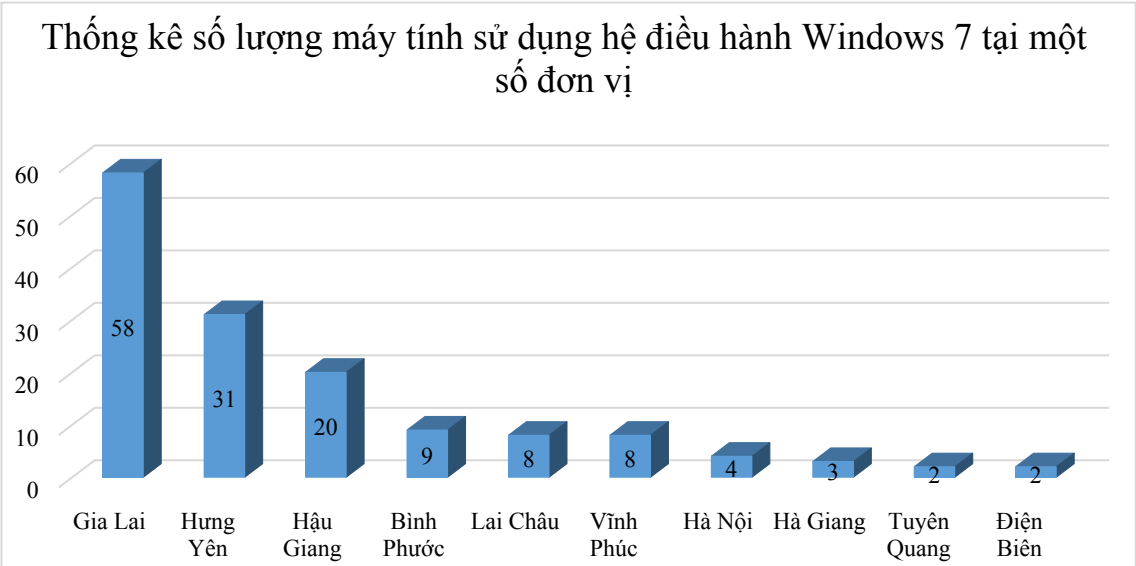
3. Thông tin giám sát, bảo đảm an toàn đường truyền mạng diện rộng (WAN) Ngành BHXH Việt Nam

Hệ thống giám sát phát hiện có 1.023 sự cố kênh truyền gây gián đoạn hoạt động, trong đó 76 sự cố kênh truyền Viettel, 43 sự cố kênh truyền VNPT, 65 sự cố thiết bị, 754 sự cố mất điện, 85 sự cố khác; 23 kênh truyền di chuyển sang trụ sở làm việc mới của BHXH tỉnh, thành phố và BHXH cấp huyện.

4. Thông tin về các điểm yếu, lỗ hổng



BHXH các tỉnh, thành phố: Điện Biên, Vĩnh Phúc, Bình Phước, Quảng Ngãi, Bến Tre, Sóc Trăng, Bạc Liêu, Gia Lai, Lai Châu, Vĩnh Long có nhiều máy tính người dùng trong mạng nội bộ chưa được cập nhật bản vá từ máy chủ quản trị tập trung của Ngành. Thông tin về các đơn vị có máy tính chưa được cập nhật bản vá từ máy chủ quản trị tại Phụ lục 5.



BHXH các tỉnh, thành phố: Gia Lai, Hưng Yên, Hậu Giang, Bình Phước, Lai Châu, Vĩnh Phúc, Hà Nội, Hà Giang, Tuyên Quang, Điện Biên còn có máy tính sử dụng hệ điều hành Windows 7. Thông tin về các đơn vị có máy tính sử dụng hệ điều hành Windows 7 tại Phụ lục 5.

Hệ thống giám sát của Trung tâm điều hành hệ thống thông tin ngành BHXH Việt Nam đã ghi nhận các bản vá chưa được cập nhật gây mất an toàn thông tin tồn tại trên nhiều máy tính đã kết nối, chia sẻ thông tin, ảnh hưởng trên diện rộng, đặc biệt có một số lỗ hổng đã và đang được các nhóm tấn công lợi dụng để thực hiện các cuộc tấn công APT với tổng số 1.746 máy tính chưa cập nhật đầy đủ các bản vá, 160 máy tính sử dụng Windows 7. Nhằm đảm bảo an toàn hệ thống, đề nghị đầu mối chuyên trách về công nghệ thông tin, an toàn thông tin tại các đơn vị phối hợp với các lực lượng ứng cứu sự cố thực hiện rà soát, xác định và tiến hành "Vá" các lỗ hổng trên hệ thống, đặc biệt là các lỗ hổng, điểm yếu hệ điều hành tại Phụ lục 6.

Hằng ngày, Trung tâm CNTT thực hiện gửi thông tin từ Hệ thống giám sát sự cố an toàn thông tin mạng cảnh báo đến địa chỉ thư điện tử công vụ của lãnh đạo phụ trách, cán bộ chuyên trách về công nghệ thông tin, an toàn thông tin để hỗ trợ phòng CNTT và bộ phận chuyên trách về ứng cứu sự cố tại các đơn vị sớm nhận biết được tình hình lây nhiễm mã độc, hoạt động của mạng máy tính ma (botnet). Thông tin từ hệ thống giám sát được sử dụng để đánh giá hiệu quả công tác phòng, chống mã độc đang triển khai tại các đơn vị. Trường hợp có thay đổi địa chỉ thư điện tử lãnh đạo phụ trách, cán bộ chuyên trách về công nghệ thông tin, an toàn thông tin cần thông báo về Trung tâm CNTT để bổ sung, cập nhật.

Trung tâm CNTT đề nghị các đơn vị thực hiện đầy đủ các giải pháp kỹ thuật đảm bảo ATTT, bảo vệ BMNN trên không gian mạng, triển khai hệ thống hạ tầng thông tin (mạng nội bộ, mạng wifi…) theo đúng thiết kế và quy hoạch của Ngành./.

Nơi nhận:
- Như trên;
- PTGĐ Phạm Lương Sơn (để b/c);
- Giám đốc (để b/c);
- Văn phòng, các đơn vị sự nghiệp trực thuộc BHXHVN;
- BHXH các tỉnh, thành phố;
- Các Phó Giám đốc;
- Các Phòng trực thuộc;
- Lưu: VT, HTA;

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

Lê Vũ Toàn

Phụ lục 1

Danh sách đơn vị có địa chỉ IP trong mạng nội bộ kết nối máy chủ CnC

Số TT	Mã tỉnh	Tên đơn vị	Số lượng IP LAN kết nối	Số lượng IP CnC kết nối	Số lượt kết nối CnC
1	G24.001	Hà Nội	294	216	19.417
2	G24.002	Hà Giang	22	20	11.268
3	G24.004	Cao Bằng	4	5	337
4	G24.006	Bắc Kạn	9	11	2.308
5	G24.008	Tuyên Quang	0	0	0
6	G24.010	Lào Cai	5	3	90
7	G24.011	Điện Biên	2	4	667
8	G24.012	Lai Châu	5	10	6.308
9	G24.014	Sơn La	7	14	494
10	G24.015	Yên Bái	2	3	311
11	G24.017	Hòa Bình	8	11	1.251
12	G24.019	Thái Nguyên	5	5	632
13	G24.020	Lạng Sơn	10	20	134.941
14	G24.022	Quảng Ninh	112	59	31.587
15	G24.024	Bắc Giang	18	13	2.964
16	G24.025	Phú Thọ	36	111	2.050
17	G24.026	Vĩnh Phúc	10	33	2.605
18	G24.027	Bắc Ninh	10	103	90.334
19	G24.030	Hải Dương	7	10	1.222
20	G24.031	Hải Phòng	17	38	2.941
21	G24.033	Hưng Yên	17	30	39.651
22	G24.034	Thái Bình	8	79	813
23	G24.035	Hà Nam	3	4	817
24	G24.036	Nam Định	6	6	690
25	G24.037	Ninh Bình	16	25	22.284
26	G24.038	Thanh Hoá	18	24	6.859
27	G24.040	Nghệ An	9	10	1.061
28	G24.042	Hà Tĩnh	7	5	90
29	G24.044	Quảng Bình	4	8	1.522
30	G24.045	Quảng Trị	36	37	21.565
31	G24.046	Thừa Thiên Huế	9	13	1.273
32	G24.048	Đà Nẵng	1	1	30

33	G24.049	Quảng Nam	16	72	7.240
34	G24.051	Quảng Ngãi	5	9	1.300
35	G24.052	Bình Định	10	18	2.811
36	G24.054	Phú Yên	4	9	1.203
37	G24.056	Khánh Hòa	6	11	1.982
38	G24.058	Ninh Thuận	14	39	10.294
39	G24.060	Bình Thuận	10	23	2.913
40	G24.062	Kon Tum	5	9	3.169
41	G24.064	Gia Lai	14	56	5.248
42	G24.066	Đăk Lăk	22	41	9.169
43	G24.067	Đăk Nông	4	4	885
44	G24.068	Lâm Đồng	8	7	1.604
45	G24.070	Bình Phước	5	8	2.279
46	G24.072	Tây Ninh	10	21	3.039
47	G24.074	Bình Dương	12	12	1.579
48	G24.075	Đồng Nai	12	17	3.043
49	G24.077	Bà Rịa - Vũng Tàu	2	5	1.010
50	G24.079	TP. Hồ Chí Minh	72	80	16.941
51	G24.080	Long An	23	59	20.890
52	G24.082	Tiền Giang	14	14	903
53	G24.083	Bến Tre	7	15	3.129
54	G24.084	Trà Vinh	6	28	4.090
55	G24.086	Vĩnh Long	4	16	4.441
56	G24.087	Đồng Tháp	8	10	446
57	G24.089	An Giang	11	22	4.030
58	G24.091	Kiên Giang	15	16	1.787
59	G24.092	Cần Thơ	5	8	1.543
60	G24.093	Hậu Giang	6	6	993
61	G24.094	Sóc Trăng	9	12	1.920
62	G24.095	Bạc Liêu	10	23	5.123
63	G24.096	Cà Mau	8	19	3.488

Phụ lục 2
Danh sách đơn vị có địa chỉ IP trong mạng nội bộ có kết nối mã độc spyware và virus

Số TT	Mã tỉnh	Tên đơn vị	Số lượng IP LAN kết nối spyware	Số lượt kết nối spyware	Số lượng IP LAN kết nối virus	Số lượt kết nối virus
1	G24.001	Hà Nội	17	3.258	0	0
2	G24.002	Hà Giang	38	100.432	4	284
3	G24.004	Cao Bằng	9	38.194	2	42
4	G24.006	Bắc Kạn	2	44	0	0
5	G24.008	Tuyên Quang	0	0	0	0
6	G24.010	Lào Cai	4	15.090	0	0
7	G24.011	Điện Biên	9	50	0	0
8	G24.012	Lai Châu	3	6	0	0
9	G24.014	Sơn La	16	3.936	8	30
10	G24.015	Yên Bái	4	1.026	0	0
11	G24.017	Hòa Bình	2	38	0	0
12	G24.019	Thái Nguyên	7	3.718	0	0
13	G24.020	Lạng Sơn	1	2	0	0
14	G24.022	Quảng Ninh	59	17.214	0	0
15	G24.024	Bắc Giang	9	836	0	0
16	G24.025	Phú Thọ	7	2.660	0	0
17	G24.026	Vĩnh Phúc	5	9.862	0	0
18	G24.027	Bắc Ninh	14	2.874	0	0
19	G24.030	Hải Dương	15	1.562	0	0
20	G24.031	Hải Phòng	7	2.284	0	0
21	G24.033	Hưng Yên	9	102.192	0	0
22	G24.034	Thái Bình	0	0	0	0
23	G24.035	Hà Nam	3	54	0	0
24	G24.036	Nam Định	4	136	0	0
25	G24.037	Ninh Bình	15	97.994	0	0
26	G24.038	Thanh Hoá	43	25.996	0	0
27	G24.040	Nghệ An	3	192	0	0
28	G24.042	Hà Tĩnh	39	4.786	1	8
29	G24.044	Quảng Bình	8	21.736	0	0
30	G24.045	Quảng Trị	5	62	0	0

31	G24.046	Thừa Thiên Huế	10	64.234	0	0
32	G24.048	Đà Nẵng	24	1.332	0	0
33	G24.049	Quảng Nam	22	694	0	0
34	G24.051	Quảng Ngãi	9	96	0	0
35	G24.052	Bình Định	2	1.048	0	0
36	G24.054	Phú Yên	1	4	0	0
37	G24.056	Khánh Hòa	0	0	0	0
38	G24.058	Ninh Thuận	1	66	0	0
39	G24.060	Bình Thuận	5	36	0	0
40	G24.062	Kon Tum	22	53.336	0	0
41	G24.064	Gia Lai	14	51.384	0	0
42	G24.066	Đăk Lăk	0	0	0	0
43	G24.067	Đăk Nông	0	0	0	0
44	G24.068	Lâm Đồng	16	114.838	0	0
45	G24.070	Bình Phước	2	8	0	0
46	G24.072	Tây Ninh	4	398	0	0
47	G24.074	Bình Dương	2	342	0	0
48	G24.075	Đồng Nai	5	56	1	4
49	G24.077	Bà Rịa - Vũng Tàu	9	416	0	0
50	G24.079	TP. Hồ Chí Minh	86	4.018	4	20
51	G24.080	Long An	5	18	0	0
52	G24.082	Tiền Giang	4	132	0	0
53	G24.083	Bến Tre	4	16	0	0
54	G24.084	Trà Vinh	0	0	0	0
55	G24.086	Vĩnh Long	4	66	0	0
56	G24.087	Đồng Tháp	3	28	0	0
57	G24.089	An Giang	21	398	0	0
58	G24.091	Kiên Giang	0	0	0	0
59	G24.092	Cần Thơ	12	6.442	0	0
60	G24.093	Hậu Giang	3	52	0	0
61	G24.094	Sóc Trăng	2	16	0	0
62	G24.095	Bạc Liêu	1	2	0	0
63	G24.096	Cà Mau	12	39.732	1	2

Phụ lục 3

Thống kê số lượng máy tính nhiễm mã độc được phát hiện tại các đơn vị

Số TT	Mã tỉnh	Tên đơn vị	Tổng số bản quyền	Số lượng máy tính bị mất kết nối	Số lượng máy đã bật tính năng bảo vệ thời gian thực	Số lượng máy tính phát hiện mã độc	Số lượng mã độc đã phát hiện
1	G24.001	Hà Nội	1440	91	1048	78	36
2	G24.002	Hà Giang	239	16	264	5	5
3	G24.004	Cao Bằng	262	5	216	13	13
4	G24.006	Bắc Kạn	213	5	152	4	4
5	G24.008	Tuyên Quang	265	10	212	5	4
6	G24.010	Lào Cai	258	10	225	12	7
7	G24.011	Điện Biên	217	2	217	4	3
8	G24.012	Lai Châu	172	3	150	9	9
9	G24.014	Sơn La	250	5	229	14	9
10	G24.015	Yên Bái	257	12	156	2	2
11	G24.017	Hòa Bình	269	19	271	3	3
12	G24.019	Thái Nguyên	309	22	192	0	0
13	G24.020	Lạng Sơn	215	4	91	21	9
14	G24.022	Quảng Ninh	389	8	217	39	10
15	G24.024	Bắc Giang	283	8	192	12	10
16	G24.025	Phú Thọ	337	11	135	14	5
17	G24.026	Vĩnh Phúc	274	3	236	14	11
18	G24.027	Bắc Ninh	246	12	213	8	6

19	G24.030	Hải Dương	365	22	361	36	21
20	G24.031	Hải Phòng	463	8	154	23	11
21	G24.033	Hưng Yên	255	1	76	18	15
22	G24.034	Thái Bình	326	10	233	30	15
23	G24.035	Hà Nam	250	11	212	11	8
24	G24.036	Nam Định	270	7	246	12	11
25	G24.037	Ninh Bình	266	5	134	13	9
26	G24.038	Thanh Hoá	568	6	371	32	23
27	G24.040	Nghệ An	538	23	469	94	37
28	G24.042	Hà Tĩnh	310	74	269	6	6
29	G24.044	Quảng Bình	256	4	147	5	4
30	G24.045	Quảng Trị	253	5	183	4	4
31	G24.046	Thừa Thiên Huế	269	7	147	3	3
32	G24.048	Đà Nẵng	191	2	240	48	29
33	G24.049	Quảng Nam	369	51	157	4	4
34	G24.051	Quảng Ngãi	295	13	281	12	7
35	G24.052	Bình Định	265	5	220	12	10
36	G24.054	Phú Yên	223	14	151	8	8
37	G24.056	Khánh Hòa	217	65	240	7	7
38	G24.058	Ninh Thuận	177	3	180	7	5
39	G24.060	Bình Thuận	226	5	229	11	7
40	G24.062	Kon Tum	218	36	86	6	6
41	G24.064	Gia Lai	294	3	168	5	5
42	G24.066	Đăk Lăk	314	6	245	18	10

43	G24.067	Đăk Nông	175	68	98	0	0
44	G24.068	Lâm Đồng	248	5	197	10	6
45	G24.070	Bình Phước	215	8	198	10	10
46	G24.072	Tây Ninh	209	3	178	3	3
47	G24.074	Bình Dương	405	16	426	9	7
48	G24.075	Đồng Nai	438	12	164	10	6
49	G24.077	Bà Rịa - Vũng Tàu	242	9	217	28	11
50	G24.079	TP. Hồ Chí Minh	1315	70	915	88	37
51	G24.080	Long An	343	19	298	134	25
52	G24.082	Tiền Giang	225	16	229	28	18
53	G24.083	Bến Tre	221	8	184	12	12
54	G24.084	Trà Vinh	235	4	220	9	9
55	G24.086	Vĩnh Long	195	18	157	10	7
56	G24.087	Đồng Tháp	262	10	269	6	6
57	G24.089	An Giang	282	14	206	13	8
58	G24.091	Kiên Giang	253	2	221	2	2
59	G24.092	Cần Thơ	215	6	167	18	8
60	G24.093	Hậu Giang	181	3	145	11	6
61	G24.094	Sóc Trăng	233	9	215	10	8
62	G24.095	Bạc Liêu	220	6	180	5	4
63	G24.096	Cà Mau	204	8	119	7	3

Phụ lục 4

Thống kê số lượng máy tính chạy tiến trình nghi ngờ mã độc (MD5/SHA256) và domain độc hại/lừa đảo trên EDR

Số TT	Mã tỉnh	Tên đơn vị	Số máy tính bị mất kết nối	Số lượng máy tính có cảnh báo tiến trình mã độc (MD5/SHA256)	Số tiến trình nghi ngờ là mã độc (MD5/SHA256)	Số lượt cảnh báo	Số lượng máy tính có kết nối domain độc hại/lừa đảo	Số lượng domain độc hại/lừa đảo	Số lượt cảnh báo
1	G24.001	Hà Nội	45	7	0	236	1	1	1
2	G24.002	Hà Giang	3	0	0	0	1	1	2
3	G24.004	Cao Bằng	3	0	0	0	0	0	0
4	G24.006	Bắc Kạn	2	0	0	0	0	0	0
5	G24.008	Tuyên Quang	3	0	2	0	0	0	0
6	G24.010	Lào Cai	4	3	0	68	0	0	0
7	G24.011	Điện Biên	3	0	0	0	0	0	0
8	G24.012	Lai Châu	6	0	0	0	0	0	0
9	G24.014	Sơn La	40	0	0	0	0	0	0
10	G24.015	Yên Bái	3	0	0	0	0	0	0
11	G24.017	Hòa Bình	11	0	1	0	0	0	0
12	G24.019	Thái Nguyên	7	2	1	7079	1	1	1
13	G24.020	Lạng Sơn	6	1	4	109407	1	1	26
14	G24.022	Quảng Ninh	3	8	0	32994	0	0	0
15	G24.024	Bắc Giang	17	0	3	0	2	1	2
16	G24.025	Phú Thọ	9	14	0	44413	1	2	26
17	G24.026	Vĩnh Phúc	3	0	0	0	1	1	1
18	G24.027	Bắc Ninh	6	0	0	0	0	0	0

19	G24.030	Hải Dương	13	0	0	0	3	3	13
20	G24.031	Hải Phòng	2	0	1	0	1	1	1
21	G24.033	Hưng Yên	3	1	0	1	1	1	1
22	G24.034	Thái Bình	55	0	0	0	0	0	0
23	G24.035	Hà Nam	3	0	0	0	0	0	0
24	G24.036	Nam Định	3	0	0	0	0	0	0
25	G24.037	Ninh Bình	5	0	0	0	1	1	1
26	G24.038	Thanh Hóa	13	0	0	0	2	3	42
27	G24.040	Nghệ An	16	0	1	0	0	0	0
28	G24.042	Hà Tĩnh	4	1	0	135	0	0	0
29	G24.044	Quảng Bình	5	0	0	0	1	1	1
30	G24.045	Quảng Trị	5	0	0	0	0	0	0
31	G24.046	Thừa Thiên Huế	6	0	0	0	0	0	0
32	G24.048	Đà Nẵng	0	0	1	0	3	2	3
33	G24.049	Quảng Nam	3	1	0	57	1	1	1
34	G24.051	Quảng Ngãi	6	0	0	0	1	1	1
35	G24.052	Bình Định	3	0	1	0	1	1	2
36	G24.054	Phú Yên	1	1	0	9914	0	0	0
37	G24.056	Khánh Hòa	5	0	0	0	2	1	2
38	G24.058	Ninh Thuận	8	0	0	0	0	0	0
39	G24.060	Bình Thuận	2	0	0	0	1	1	2
40	G24.062	Kon Tum	1	0	1	0	0	0	0
41	G24.064	Gia Lai	1	1	0	10	2	1	2
42	G24.066	Đắk Lắk	5	0	0	0	1	1	1
43	G24.067	Đắk Nông	3	0	0	0	0	0	0
44	G24.068	Lâm Đồng	3	0	0	0	2	1	2

45	G24.070	Bình Phước	3	0	0	0	0	0	0
46	G24.072	Tây Ninh	8	0	0	0	1	1	1
47	G24.074	Bình Dương	13	0	1	0	2	1	3
48	G24.075	Đồng Nai	2	1	1	2902	1	1	1
49	G24.077	Bà Rịa - Vũng Tàu	5	1	3	1	0	0	0
50	G24.079	TP. Hồ Chí Minh	24	3	2	2776	2	1	2
51	G24.080	Long An	2	2	0	2	1	1	2
52	G24.082	Tiền Giang	1	0	0	0	2	1	2
53	G24.083	Bến Tre	3	0	0	0	1	1	1
54	G24.084	Trà Vinh	6	0	1	0	1	1	1
55	G24.086	Vĩnh Long	5	1	0	31	0	0	0
56	G24.087	Đồng Tháp	3	0	0	0	1	1	2
57	G24.089	An Giang	4	0	0	0	1	1	1
58	G24.091	Kiên Giang	5	0	0	0	2	2	4
59	G24.092	Cần Thơ	1	0	0	0	0	0	0
60	G24.093	Hậu Giang	1	0	0	0	2	1	2
61	G24.094	Sóc Trăng	4	0	0	0	1	1	1
62	G24.095	Bạc Liêu	4	0	0	0	0	0	0
63	G24.096	Cà Mau	2	0	0	0	0	0	0

Phụ lục 5

Thống kê sử dụng phần mềm quản lý và cập nhật bản vá tại các đơn vị

Số TT	Mã định danh	Tên đơn vị	Tổng số máy tính[3]	Số máy tính cài đặt[4]	Số máy tính mất kết nối	Số máy tính chưa cập nhật bản vá	Số máy tính sử dụng HĐH Windows 7
1	G24.001	Hà Nội	1586	673	7	31	4
2	G24.002	Hà Giang	247	227	21	22	3
3	G24.004	Cao Bằng	353	224	18	13	0
4	G24.006	Bắc Kạn	246	170	4	21	0
5	G24.008	Tuyên Quang	228	202	7	30	2
6	G24.010	Lào Cai	241	229	10	6	1
7	G24.011	Điện Biên	125	234	9	104	2
8	G24.012	Lai Châu	192	186	23	44	8
9	G24.014	Sơn La	342	329	30	32	0
10	G24.015	Yên Bái	263	167	14	19	0
11	G24.017	Hòa Bình	337	292	19	13	0
12	G24.019	Thái Nguyên	374	184	42	30	1
13	G24.020	Lạng Sơn	234	205	26	16	0
14	G24.022	Quảng Ninh	283	235	32	29	0
15	G24.024	Bắc Giang	261	224	12	22	1
16	G24.025	Phú Thọ	348	174	29	13	0
17	G24.026	Vĩnh Phúc	266	207	5	104	8
18	G24.027	Bắc Ninh	240	149	2	7	0
19	G24.030	Hải Dương	444	343	1	35	0
20	G24.031	Hải Phòng	480	291	35	23	0
21	G24.033	Hưng Yên	238	160	10	30	31
22	G24.034	Thái Bình	334	288	35	7	0
23	G24.035	Hà Nam	254	232	13	18	0
24	G24.036	Nam Định	292	267	26	14	0
25	G24.037	Ninh Bình	230	204	21	7	0
26	G24.038	Thanh Hóa	563	401	26	30	0
27	G24.040	Nghệ An	555	468	6	12	0
28	G24.042	Hà Tĩnh	292	245	56	14	0
29	G24.044	Quảng Bình	259	229	17	14	0
30	G24.045	Quảng Trị	267	214	12	16	0
31	G24.046	Thừa Thiên Huế	273	206	34	15	0

[3] Số liệu tổng hợp trên phần mềm quản lý thiết bị

[4] Số liệu tổng hợp trên hệ thống quản trị tập trung của Ngành. Thông tin liên hệ hỗ trợ: Trần Thái Sơn: 0904881993, Hotline NOC: 0984391786

32	G24.048	Đà Nẵng	297	244	31	8	1
33	G24.049	Quảng Nam	362	346	64	10	0
34	G24.051	Quảng Ngãi	289	280	23	90	1
35	G24.052	Bình Định	241	192	2	28	0
36	G24.054	Phú Yên	231	178	28	15	0
37	G24.056	Khánh Hòa	227	258	9	26	0
38	G24.058	Ninh Thuận	185	172	19	26	0
39	G24.060	Bình Thuận	230	214	10	27	1
40	G24.062	Kon Tum	226	182	9	21	1
41	G24.064	Gia Lai	354	158	12	51	58
42	G24.066	Đắk Lắk	319	294	26	14	0
43	G24.067	Đắk Nông	198	164	23	13	0
44	G24.068	Lâm Đồng	246	202	12	25	2
45	G24.070	Bình Phước	227	200	21	91	9
46	G24.072	Tây Ninh	211	222	19	22	0
47	G24.074	Bình Dương	343	406	47	17	0
48	G24.075	Đồng Nai	416	324	25	13	0
49	G24.077	Bà Rịa - Vũng Tàu	240	211	20	16	0
50	G24.079	TP. Hồ Chí Minh	1421	1045	115	5	0
51	G24.080	Long An	281	280	34	28	0
52	G24.082	Tiền Giang	246	216	14	5	0
53	G24.083	Bến Tre	226	182	22	86	0
54	G24.084	Trà Vinh	207	209	0	21	0
55	G24.086	Vĩnh Long	188	122	17	44	2
56	G24.087	Đồng Tháp	255	250	19	29	1
57	G24.089	An Giang	256	189	17	6	0
58	G24.091	Kiên Giang	224	236	14	38	2
59	G24.092	Cần Thơ	168	180	26	22	0
60	G24.093	Hậu Giang	173	160	2	19	20
61	G24.094	Sóc Trăng	224	215	12	77	0
62	G24.095	Bạc Liêu	198	176	9	54	0
63	G24.096	Cà Mau	168	206	42	8	1

Phụ lục 6

Danh sách điểm yếu, lỗ hổng hệ điều hành Windows 10 đã có bản vá cập nhật

Số TT	Mã bản vá	Mức độ	Thông tin chi tiết về bản vá
1	MS21-AUG12	Critical	2021-08 Servicing Stack Update for Windows 10 Version 21H1 for x64-based Systems (KB5005260)
2	MS22-JAN3	Critical	2022-01 Cumulative Update for Windows 10 Version 21H1 for x64-based Systems (KB5009543) (CVE-2021-22947) (CVE-2021-22947) (CVE-2022-21919) (CVE-2022-21836) (CVE-2022-21874)
3	MS22-JAN3	Critical	2022-01 Cumulative Update for Windows 10 Version 20H2 for x64-based Systems (KB5009543) (CVE-2021-22947) (CVE-2021-22947) (CVE-2022-21919) (CVE-2022-21836) (CVE-2022-21874)
4	MS21-AUG12	Critical	2021-08 Servicing Stack Update for Windows 10 Version 2004 for x64-based Systems (KB5005260)
5	MS21-DEC3	Critical	2021-12 Cumulative Update for Windows 10 Version 2004 for x64-based Systems (KB5008212) (CVE-2021-43240) (CVE-2021-41333) (CVE-2021-43883) (CVE-2021-43893)
6	MS20-NOV12	Critical	2020-11 Servicing Stack Update for Windows 10 Version 1903 for x64-based Systems (KB4586863)
7	MS20-DEC3	Critical	2020-12 Cumulative Update for Windows 10 Version 1903 for x64-based Systems (KB4592449)
8	MS22-JAN3	Critical	2022-01 Cumulative Update for Windows 10 Version 21H2 for x64-based Systems (KB5009543) (CVE-2021-22947) (CVE-2021-22947) (CVE-2022-21919) (CVE-2022-21836) (CVE-2022-21874)
9	MS21-DEC3	Critical	2021-12 Cumulative Update for Windows 10 Version 21H1 for x64-based Systems (KB5008212) (CVE-2021-43240) (CVE-2021-41333) (CVE-2021-43883) (CVE-2021-43893)
10	MS21-AUG12	Critical	2021-08 Servicing Stack Update for Windows 10 Version 20H2 for x64-based Systems (KB5005260)
11	MS21-AUG12	Critical	2021-08 Servicing Stack Update for Windows 10 Version 1809 for x64-based Systems (KB5005112)
12	MS22-JAN3	Critical	2022-01 Cumulative Update for Windows 10 Version 1809 for x64-based Systems (KB5009557) (CVE-2021-22947) (CVE-2021-22947) (CVE-2022-21919) (CVE-2022-21836) (CVE-2022-21839) (CVE-2022-21874)
13	MS21-AUG12	Critical	2021-08 Servicing Stack Update for Windows 10 Version 2004 for x86-based Systems (KB5005260)
14	MS21-DEC3	Critical	2021-12 Cumulative Update for Windows 10 Version 2004 for x86-based Systems (KB5008212) (CVE-2021-43240) (CVE-2021-41333) (CVE-2021-43883) (CVE-2021-43893)
15	MS20-JUL12	Critical	2020-07 Servicing Stack Update for Windows 10 Version 1709 for x64-based Systems (KB4565553)

16	MS20-OCT3	Critical	2020-10 Cumulative Update for Windows 10 Version 1709 for x64-based Systems (KB4580328) (CVE-2020-16898)
17	MS21-NOV3	Critical	2021-11 Cumulative Update for Windows 10 Version 2004 for x64-based Systems (KB5007186) (CVE-2021-41371) (CVE-2021-38631)
18	MS21-DEC3	Critical	2021-12 Cumulative Update for Windows 10 Version 21H2 for x64-based Systems (KB5008212) (CVE-2021-43240) (CVE-2021-41333) (CVE-2021-43883) (CVE-2021-43893)
19	MS21-AUG12	Critical	2021-08 Servicing Stack Update for Windows 10 Version 20H2 for x86-based Systems (KB5005260)
20	MS22-JAN3	Critical	2022-01 Cumulative Update for Windows 10 Version 20H2 for x86-based Systems (KB5009543) (CVE-2021-22947) (CVE-2021-22947) (CVE-2022-21919) (CVE-2022-21836) (CVE-2022-21874)
21	MS21-NOV3	Critical	2021-11 Cumulative Update for Windows 10 Version 20H2 for x64-based Systems (KB5007186) (CVE-2021-41371) (CVE-2021-38631)
22	MS20-NOV12	Critical	2020-11 Servicing Stack Update for Windows 10 Version 1903 for x86-based Systems (KB4586863)
23	MS20-DEC3	Critical	2020-12 Cumulative Update for Windows 10 Version 1903 for x86-based Systems (KB4592449)
24	MS21-DEC3	Critical	2021-12 Cumulative Update for Windows 10 Version 20H2 for x64-based Systems (KB5008212) (CVE-2021-43240) (CVE-2021-41333) (CVE-2021-43883) (CVE-2021-43893)
25	MS21-NOV3	Critical	2021-11 Cumulative Update for Windows 10 Version 21H1 for x64-based Systems (KB5007186) (CVE-2021-41371) (CVE-2021-38631)
26	MS21-OCT3	Critical	2021-10 Cumulative Update for Windows 10 Version 2004 for x64-based Systems (KB5006670) (CVE-2021-40449) (CVE-2021-40469) (CVE-2021-41335) (CVE-2021-41338)
27	MS21-OCT3	Critical	2021-10 Cumulative Update for Windows 10 Version 20H2 for x64-based Systems (KB5006670) (CVE-2021-40449) (CVE-2021-40469) (CVE-2021-41335) (CVE-2021-41338)
28	MS21-OCT3	Critical	2021-10 Cumulative Update for Windows 10 Version 21H1 for x64-based Systems (KB5006670) (CVE-2021-40449) (CVE-2021-40469) (CVE-2021-41335) (CVE-2021-41338)
29	MS21-OCT3	Critical	2021-10 Cumulative Update for Windows 10 Version 1809 for x64-based Systems (KB5006672) (CVE-2021-40449) (CVE-2021-40469) (CVE-2021-41335) (CVE-2021-41338)
30	MS21-NOV3	Critical	2021-11 Cumulative Update for Windows 10 Version 1809 for x64-based Systems (KB5007206) (CVE-2021-41371) (CVE-2021-38631)
31	MS21-NOV3	Critical	2021-11 Cumulative Update for Windows 10 Version 20H2 for x86-based Systems (KB5007186) (CVE-2021-41371) (CVE-2021-38631)

32	MS22-JAN3	Critical	2022-01 Cumulative Update for Windows 10 Version 21H2 for x86-based Systems (KB5009543) (CVE-2021-22947) (CVE-2021-22947) (CVE-2022-21919) (CVE-2022-21836) (CVE-2022-21874)
33	MS21-DEC3	Critical	2021-12 Cumulative Update for Windows 10 Version 20H2 for x86-based Systems (KB5008212) (CVE-2021-43240) (CVE-2021-41333) (CVE-2021-43883) (CVE-2021-43893)
34	MS22-JAN3	Critical	2022-01 Cumulative Update for Windows 10 Version 1607 for x64-based Systems (KB5009546) (CVE-2022-21919) (CVE-2022-21836) (CVE-2022-21874)
35	MS22-JAN3	Critical	2022-01 Cumulative Update for Windows 10 Version 1909 for x64-based Systems (KB5009545) (CVE-2021-22947) (CVE-2021-22947) (CVE-2022-21919) (CVE-2022-21836) (CVE-2022-21874)
36	MS21-SEP12	Critical	2021-09 Servicing Stack Update for Windows 10 Version 1607 for x64-based Systems (KB5005698)
37	MS21-DEC3	Critical	2021-12 Cumulative Update for Windows 10 Version 21H2 for x86-based Systems (KB5008212) (CVE-2021-43240) (CVE-2021-41333) (CVE-2021-43883) (CVE-2021-43893)
38	MS21-DEC3	Critical	2021-12 Cumulative Update for Windows 10 Version 1809 for x64-based Systems (KB5008218) (CVE-2021-43883) (CVE-2021-43893)
39	MS21-MAY12	Critical	2021-05 Servicing Stack Update for Windows 10 Version 1803 for x64-based Systems (KB5003364)
40	MS21-MAY3	Critical	2021-05 Cumulative Update for Windows 10 Version 1803 for x64-based Systems (KB5003174)
41	MS21-AUG12	Critical	2021-08 Servicing Stack Update for Windows 10 Version 1909 for x64-based Systems (KB5005412)
42	MS21-AUG12	Critical	2021-08 Servicing Stack Update for Windows 10 Version 21H1 for x86-based Systems (KB5005260)
43	MS21-OCT3	Critical	2021-10 Cumulative Update for Windows 10 Version 21H1 for x86-based Systems (KB5006670) (CVE-2021-40449) (CVE-2021-40469) (CVE-2021-41335) (CVE-2021-41338)